SSH Secure Shell for Workstations Windows Client Version 3.2 User Manual

May, 2002

© 2002 SSH Communications Security Corp.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corp.

ssh® is a registered trademark of SSH Communications Security Corp in the United States and in certain other jurisdictions. SSH2, the SSH logo, IPSEC Express, SSH Certifier, SSH Sentinel, SSH NAT Traversal, IPSEC on silicon, Hypermode, SSH Accession, SSH Token Master, SSH Secure Shell, QuickSec, and Making the Internet Secure are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. All other names and marks are property of their respective owners. This product may be covered, among others, by the following U.S. Patents: 6,253,321. Other patents pending.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

SSH Communications Security Corp.
Fredrikinkatu 42
FIN-00100 Helsinki
FINLAND

SSH Communications Security Inc.
1076 East Meadow Circle
Palo Alto, CA 94303
USA

SSH Communications Security K.K.
House Hamamatsu-cho Bldg. 5F
2-7-1 Hamamatsu-cho, Minato-ku
Tokyo 105-0013, JAPAN

http://www.ssh.com/

Tel: +358 20 500 7030 (Finland), +1 650 251 2700 (USA), +81 3 3459 6830 (Japan)
Fax: +358 20 500 7031 (Finland), +1 650 251 2701 (USA), +81 3 3459 6825 (Japan)

Contents

1 Introduction **15**

1.1 Network Security Risks 15

1.1.1 Security of Internet Protocol 16

1.2 Different Secure Shell Versions 16

1.3 SSH2 Protocol Features 17

1.4 New Features 18

1.5 System Requirements 19

1.6 Desktop Icons 19

1.7 Support 19

2 Configuration **21**

2.1 Saving Settings 21

2.1.1 Multiple Settings Files 22

2.2 Loading Settings 22

2.3 Profile Settings 23

2.3.1 Connection 24

2.3.2 Cipher List 26

2.3.3 Authentication 27

2.3.4 Colors 30

2.3.5 Keyboard 32

 © 2002 SSH Communications Security Corp.

2.3.6 Keymap Editor 33
2.3.7 Tunneling 35
2.3.8 File Transfer 40
2.3.9 Favorites 41
2.4 Global Settings 42
2.4.1 Appearance 42
2.4.2 Font 45
2.4.3 Colors 45
2.4.4 Messages 46
2.4.5 User Authentication 46
2.4.6 Keys 48
2.4.7 Certificates 50
2.4.8 Certificate Enrollment Wizard 52
2.4.9 SSH Accession 55
2.4.10 PKCS #11 56
2.4.11 Configuration 57
2.4.12 PKCS #11 Provider 58
2.4.13 Server Authentication 60
2.4.14 Host Keys 61
2.4.15 CA Certificates 62
2.4.16 LDAP Servers 64
2.4.17 File Transfer 65
2.4.18 Advanced 69
2.4.19 Mode 70
2.4.20 Local Favorites 72
2.4.21 Firewall 73

2.4.22 Security 74
2.4.23 Printing 75
2.5 Customize 76

3 Connecting 79

3.1 Quick Connect 79
3.2 Profiles 80
3.2.1 Add Profile 80
3.2.2 Edit Profiles 80
3.3 Key Generation 83
3.3.1 Key Generation Wizard 83
3.3.2 Key Generation - Start 83
3.3.3 Key Generation - Key Properties 83
3.3.4 Key Generation - Generation 85
3.3.5 Key Generation - Enter Passphrase 85
3.3.6 Key Generation - Finish 87
3.4 Connecting to a Remote Host Computer 87
3.4.1 Host Identification Dialog 88
3.4.2 Connect to Remote Host Dialog 89
3.5 Uploading Your Public Key 91
3.5.1 Manually Copying the Key File 92
3.5.2 Manually Editing the Authorization File 93
3.6 Using Public-Key Authentication 94
3.7 Command Line Options 95

4 Terminal Window 97

4.1 Terminal Window Title Bar 97

 © 2002 SSH Communications Security Corp.

4.2 Terminal Window Status Bar 98

4.3 Terminal Window Shortcut Menu 99

5 File Transfer **101**

5.1 File Transfer Window Layout 102

5.1.1 File Transfer Title Bar 102

5.1.2 File Transfer Menu Bar 102

5.1.3 File Transfer Toolbars 103

5.1.4 File Transfer Status Bar 103

5.1.5 Contents of the File Transfer Window 104

5.1.6 Local View 106

5.1.7 Local Folder View 106

5.1.8 Remote View 106

5.1.9 Remote Folder View 106

5.1.10 Transfer View 107

5.2 Navigating in the File Transfer Window 109

5.2.1 Drag And Drop Operations 109

5.3 File Transfer Shortcut Menus 109

5.3.1 Local View 110

5.3.2 Remote View 111

5.3.3 Transfer Page 112

5.3.4 Queue Page 113

5.4 Differences From *Windows Explorer* 114

5.5 Downloading Files 114

5.5.1 Download - Select Folder Dialog 115

5.6 Uploading Files 115

5.6.1 Upload - Select Files Dialog 116

5.7 File Properties 117

6 Toolbar Reference 119

6.1 Configuring Toolbars 119

6.1.1 Moving Toolbars 120

6.1.2 Moving Toolbar Buttons 120

6.1.3 Permanent Toolbar Changes 120

6.2 Save Settings 120

6.3 Print 121

6.4 Print Preview 121

6.5 Connect 122

6.6 Disconnect 123

6.7 Copy 123

6.8 Paste 124

6.9 Paste Selection 124

6.10 Find 125

6.11 New Terminal Window 126

6.12 New File Transfer Window 127

6.13 Settings 127

6.14 Contents 127

6.15 Get Help On 127

6.16 File Transfer Specific Toolbar Buttons 127

6.16.1 Download Dialog 128

6.16.2 Upload Dialog 128

6.16.3 Toggle Transfer View 128

6.16.4 Large Icons 128

6.16.5 Small Icons 128

 © 2002 SSH Communications Security Corp.

6.16.6 List . . . 128
6.16.7 Details . . . 129
6.16.8 ASCII . . . 129
6.16.9 Binary . . . 129
6.16.10 Auto Select . . . 129
6.16.11 Cancel Transfer . . . 129
6.17 Profiles Bar . . . 129
6.18 File Bar . . . 130
6.18.1 Show/Hide Local Folders . . . 130
6.18.2 Local Home . . . 130
6.18.3 Up . . . 130
6.18.4 Refresh Local . . . 130
6.18.5 New Local Folder . . . 131
6.18.6 Delete Local . . . 131
6.18.7 Local Favorites . . . 131
6.18.8 Add . . . 131
6.18.9 Show/Hide Remote Folders . . . 131
6.18.10 Remote Home . . . 131
6.18.11 Up . . . 131
6.18.12 Refresh Remote . . . 132
6.18.13 New Remote Folder . . . 132
6.18.14 Delete Remote . . . 132
6.18.15 Remote Favorites . . . 132
6.18.16 Add . . . 132

7 Menu Reference **133**

7.1 Configuring Menus . . . 133

7.1.1 Moving Menus 133
7.1.2 Permanent Menu Changes 134
7.2 File Menu 134
7.2.1 Save Settings 134
7.2.2 Save Layout 134
7.2.3 Quick Connect 134
7.2.4 Profiles 134
7.2.5 Print 135
7.2.6 Print Preview 135
7.2.7 Page Setup 135
7.2.8 Log Session 135
7.2.9 Connect 135
7.2.10 Disconnect 136
7.2.11 Exit 136
7.3 Edit Menu 136
7.3.1 Copy 136
7.3.2 Paste 137
7.3.3 Paste Selection 137
7.3.4 Select All 137
7.3.5 Select Screen 138
7.3.6 Select None 138
7.3.7 Find 138
7.3.8 Settings 138
7.4 Terminal Window View Menu Options 138
7.4.1 Toolbar 139
7.4.2 Status Bar 139

 © 2002 SSH Communications Security Corp.

7.4.3 Profiles Bar . . . 139
7.4.4 Customize . . . 139
7.4.5 Reset Toolbars . . . 139
7.4.6 Reset Terminal . . . 139
7.5 File Transfer View Menu Options . . . 139
7.5.1 Toolbar . . . 140
7.5.2 Profiles Bar . . . 140
7.5.3 File Bar . . . 140
7.5.4 Status Bar . . . 140
7.5.5 Local View . . . 140
7.5.6 Transfer View . . . 140
7.5.7 Customize . . . 140
7.5.8 Reset Toolbars . . . 141
7.5.9 Large Icons . . . 141
7.5.10 Small Icons . . . 141
7.5.11 List . . . 141
7.5.12 Details . . . 141
7.5.13 Arrange Icons . . . 142
7.5.14 Show Root Directory . . . 142
7.5.15 Show Hidden Files . . . 142
7.5.16 Refresh . . . 142
7.6 Operation Menu . . . 143
7.6.1 Open . . . 143
7.6.2 Upload . . . 143
7.6.3 Download . . . 143
7.6.4 Upload Dialog . . . 143

7.6.5 Download Dialog 143
7.6.6 Cancel 144
7.6.7 Up 144
7.6.8 Home 144
7.6.9 Go To Folder 144
7.6.10 New Folder 144
7.6.11 Delete 144
7.6.12 Rename 145
7.6.13 Properties 145
7.6.14 File Transfer Mode 145
7.7 Window Menu 146
7.7.1 New Terminal 146
7.7.2 New File Transfer 146
7.7.3 New Terminal in Current Directory 146
7.7.4 New File Transfer in Current Directory 147
7.7.5 New Windows Explorer 147
7.7.6 Close 147
7.7.7 Close All Others 147
7.8 Help Menu 147
7.8.1 Contents 147
7.8.2 Get Help On 148
7.8.3 SSH on the Web 148
7.8.4 Troubleshooting 148
7.8.5 Debugging 149
7.8.6 Import License File 151
7.8.7 About Secure Shell 151

 © 2002 SSH Communications Security Corp.

8 Advanced Information 153

8.1 SSH2 Functionality 153

8.1.1 Host Keys 155

8.1.2 Security Properties 155

8.2 Public-Key Infrastructure (PKI) 155

8.2.1 CA 156

8.2.2 Certificate Enrollment 157

8.2.3 Certificate Revocation 157

8.2.4 Directory Services 158

8.3 Using Certificate Authentication 158

8.3.1 PKCS #11 159

8.4 Keyboard-Interactive Authentication 159

8.4.1 Overview 159

9 Troubleshooting 161

9.1 Error Dialogs At Startup 161

9.1.1 Evaluation Period Ending 161

9.1.2 Expiration 162

9.1.3 Failed To Read Keymap File 162

9.1.4 File Open Error 163

9.1.5 Keymap Error 163

9.1.6 Your License Has Expired 163

9.2 Error Dialogs During Operation 164

9.2.1 Authentication Failure 164

9.2.2 Confirm Disconnect 164

9.2.3 Confirm File Overwrite 165

9.2.4 Connection Failure 165

9.2.5 Disconnected; Authentication Error 166
9.2.6 Disconnection 166
9.2.7 Enter Passcode 167
9.2.8 Enter Passphrase For Private Key 167
9.2.9 Enter PIN 167
9.2.10 Error Renaming 167
9.2.11 Failed To Create An Incoming Tunnel 167
9.2.12 Host Identification 168
9.2.13 Host Identification Failed 168
9.2.14 New PIN 169
9.2.15 PAM Response 169
9.2.16 Password Needed for PFX Integrity Check 169
9.2.17 The Remote Host Uses SSH1 Protocol 169
9.2.18 Wrong Passphrase 170
9.2.19 Wrong Password - Enter Again 170
9.3 PKCS #11 Keys 170
9.3.1 Signing error 170
9.4 SSH1 Specific Error Messages 171
9.4.1 Unexpected EOF 171

A Appendices **173**

A.1 SSH2 173
A.2 SCP2 174
A.2.1 SCP2 Syntax 175
A.2.2 SCP2 Return Values 176
A.3 SFTP2 176
A.3.1 SFTP2 Commands 177

 © 2002 SSH Communications Security Corp.

A.3.2 SFTP2 Command Interpretation 179

A.4 `ssh-keygen2` 180

A.5 Frequently Asked Questions 181

Chapter 1

Introduction

The SSH Secure Shell for Workstations Windows client (SSH2 client) is a program that allows secure network services over an insecure network.

SSH Secure Shell for Workstations Windows Client replaces other, insecure terminal applications, such as Telnet and FTP. It allows you to securely login to remote host computers, to execute commands safely on a remote computer, and to provide secure encrypted and authenticated communications between two hosts in an untrusted network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel, expanding SSH Secure Shell's usability even further.

SSH Secure Shell with its array of unmatched security features is an essential tool for today's network environment. It is a powerful guardian against the numerous security hazards that threaten network communications.

1.1 Network Security Risks

The open architecture of Internet Protocol (IP) makes it a highly efficient, cost-effective, and flexible communications protocol for local and global communications. It has been widely adopted, not only on the global Internet, but also on the internal networks of large corporations.

Internet Protocol was designed to be highly reliable against random network errors. However, it was not designed to be secure against a malicious attacker. In fact, it is vulnerable to a number of well-known attacks. This is preventing it from being used to its fullest for business and other purposes involving confidential or mission-critical data.

 © 2002 SSH Communications Security Corp.

1.1.1 Security of Internet Protocol

The IP protocol suite, including TCP/IP, was designed to provide reliable and scalable communications over real-world networks. It has served this goal well. However, it was designed twenty years ago in a world where the Internet consisted of a few hundred closely controlled hosts. The situation has changed. The Internet now connects tens of millions of computers, controlled by millions of individuals and organizations. The core network itself is administered by thousands of competing operators, and the network spans the whole globe, connected by fibers, leased lines, dialup modems, and mobile phones.

The phenomenal growth of the Internet has peaked the interest of businesses, military organizations, governments, and criminals. Suddenly, networks are changing the way business is done. They have changed the nature of trade and distribution networks, and the way individual people communicate with each other.

This upsurge of business communications, scientific communications and political communications on the Internet has also brought out negative elements. Criminals are looking for ways of getting a cut of the emerging business. Industrial espionage has become a reality. Intelligence agencies are showing growing interest towards networked communications, and they often exchange information with domestic commercial interest and political groups. Crackers, exchanging information and source code, make attacks that ten years ago were thought to be only within the reach of superpowers' intelligence agencies.

Consequently, the IP protocol, while very tolerant of random errors, is vulnerable to malicious attacks. The most common types of attacks include:

- Eavesdropping on a transmission, for example, looking for passwords, credit card numbers, or business secrets.
- Hijacking, or taking over a communication in such a way that the attacker can inspect and modify any data being transmitted between the communicating parties.
- IP spoofing, or faking network addresses or host names in order to fool access control mechanisms based on them or to redirect connections to a fake server.

The SSH2 protocol is designed to protect network communications against security hazards like these.

1.2 Different Secure Shell Versions

Several different Secure Shell client and server versions exist. The different versions use different implementations of the SSH protocol.

SSH Secure Shell for Workstations Windows client uses the Secure Shell protocol version 2 (SSH2), but also supports connections to Secure Shell version 1 (SSH1) servers. Note, however, that Secure Shell version 2 (SSH2) is a more advanced protocol than the legacy version SSH1. For more information on the implications of using an SSH1 connection, see the SSH web site `http://www.ssh.com/products/ssh/advisories/statement.cfm`.

Note: SSH Communications Security has deprecated the SSH1 protocol and does not recommend using it. For more information, see `http://www.ssh.com/products/ssh/cert/deprecation.cfm`.

The SSH2 protocol provides a set of radical improvements to SSH1. These improvements include:

- A much better understood and more secure protocol.
- A new design which requires much less code to be run with administrative privileges.
- Totally rewritten code that improves security.
- New routines for cryptography and mathematics, resulting in considerable improvements in speed.
- Support for multiple public key algorithms, including RSA, DSA and Diffie-Hellman key exchange.
- Easy to use file transfers using the integrated file transfer agent in SSH Secure Shell for Workstation Windows client, and the scp2 (secure file copy) and sftp2 (secure file transfer protocol) command line applications.

1.3 SSH2 Protocol Features

The SSH2 protocol contains the following features:

- Secure terminal sessions utilizing secure encryption.
- Full, secure replacement for FTP and Telnet, as well as the UNIX r-series of commands: `rlogin`, `rsh`, `rcp`, `rexec`.
- Multiple high security algorithms and strong authentication methods that prevent such security threats as identity spoofing and man-in-the-middle attacks.
- Multiple ciphers for encryption, including e.g. 3DES, Blowfish and AES.
- Password, public key, certificate, smart card, PAM and SecurID authentication methods.
- Transparent and automatic tunneling of X11 connections and arbitrary TCP/IP-based applications, such as e-mail.
- Automatic and secure authentication of both ends of connection. Both the server and the client are authenticated to prevent identity spoofing, Trojan horses, etc.
- Unique secure file transfer interface (SFTP) fully integrated in the client software.
- Multiple channels that allow you to have multiple terminal windows and file transfers going through one secure and authenticated connection.

 © 2002 SSH Communications Security Corp.

1.4 New Features

This version of SSH Secure Shell for Workstation Windows client contains several new features and enhancements.

Some of the most notable new features of SSH Secure Shell version 3.2 are the following:

Address bar

The current remote address is conveniently displayed in the File Transfer window, and can be used to quickly change the remote directory.

ASCII transfer configuration

Different settings for transferring ASCII files can now be configured.

Favorite folders

Both local and remote views have a list of favorite folders, making routine operations faster.

Full drag and drop support

Files can be copied to and from the local and remote machines and the Windows desktop simply by dragging and dropping.

Keyboard-Interactive

Authentication using Keyboard-Interactive (Generic Message Exchange) is now supported.

Local view

Also the local files can be displayed in the file transfer window, which makes file synchronization easy.

Multiple simultaneous transfers

Several files can now be transferred at the same time in a single window.

Save layout

The window layout and positions can now be saved separately from connection settings.

SOCKS5 partially supported

The most essential SOCKS version 5 operations are now supported. (SOCKS5 authentication or encryption functionality is not supported.)

SSH Accession Lite

A 'lite' version of the SSH Accession software is now included in the distribution.

Transfer view

Customized file lists for uploading and downloading can be created with simple drag and drop operations.

Various bug fixes

This version also contains fixes for various minor bugs found in previous releases.

1.5 System Requirements

The SSH Secure Shell for Workstation Windows client does not have any special hardware or software requirements. Any computer capable of running a current version of the Microsoft Windows operating system (Windows 95 (OSR2.1), Windows 98 or 98 SE, Windows Me, Windows NT 4 (with Service Pack 5 or 6 installed), Windows 2000 (with Service Pack 1 or 2 installed), or Windows XP), and equipped with a functional connection to a remote host computer can be used.

The SSH Secure Shell for Workstations Windows client installation requires about 4 megabytes of disk space. Note that the Secure Shell client will save each user's settings in that particular user's personal directory.

1.6 Desktop Icons

When you have installed the SSH Secure Shell for Workstations Windows client, you will have two separate program icons on the Windows desktop as well as in the Windows Start menu (by default under **Start** -> **Programs** -> **SSH Secure Shell**).

The SSH Secure Shell Client icon and the SSH Secure File Transfer Client icon both start the same application, SSH Secure Shell for Workstations Windows client. The difference between the icons is that they use different settings files. The Secure Shell Client icon uses a settings file called `default.ssh2`, and the Secure File Transfer icon uses a settings file called `defaultsftp.ssh2`.

By default the settings files have been configured so that they open the appropriate SSH Secure Shell for Workstations window, either the terminal window or the SSH Secure File Transfer window. If you want to change the default configuration, you can save your settings by using the **Save Settings** option from the **File** menu.

You can also save the window position by using the **Save Layout** option from the **File** menu. If you open the SSH Secure File Transfer client by clicking the appropriate icon, then open a terminal window or two, and then save the layout, the 'extra' terminal windows will appear the next time you click the SSH Secure File Transfer Client icon. If you then close the File Transfer window and save your settings again, the next time you will see no File Transfer window at all.

Do not be alarmed by this - you can always open a new terminal or File Transfer window by clicking the appropriate toolbar button or selecting the appropriate menu item. If you then save your settings again, the new window positions will be used as default values for new connections.

For more information saving the current settings, see section 2.1 (Saving Settings).

1.7 Support

The most current version of the SSH Secure Shell for Workstations Windows client online help is available on the SSH Web pages: `http://www.ssh.com/products/ssh/winhelp/`.

 © 2002 SSH Communications Security Corp.

Frequently asked questions specific to the SSH Secure Shell Windows client are answered in the SSH Secure Shell FAQ: `http://www.ssh.com/faq`.

If the product documentation and the FAQ do not answer your questions and you have purchased the software, you can contact SSH Secure Shell Technical Support. Use the online support form available at `http://www.ssh.com/support/ssh` for support requests and `http://www.ssh.com/support/ssh/bug-report.cfm` for bug reports.

Please see the SSH Web site (`http://www.ssh.com/support/ssh/support_offering.cfm`) for more information on the terms and conditions of obtaining technical support for SSH Secure Shell from SSH Communications Security.

Chapter 2

Configuration

Before establishing a connection to a remote host computer, you should first check your connection settings. The connection settings can be changed by using the **Profiles** option of the profiles toolbar (see section 3.2 (Profiles)), or alternatively by using the **Settings** option (see section 6.13 (Settings), found on the toolbar and the **Edit** menu).

The **Profiles** dialog can be used to configure the profile settings that are associated with a single remote host computer. With the **Settings** dialog you can control also the global settings that affect all connections.

To open the **Settings** dialog, click the **Settings** button on the toolbar or select the **Settings** option from the **Edit** menu.

The different settings categories are visible on the left hand side of the **Settings** dialog as a tree structure. Branches that have a plus sign (+) next to them can be expanded by clicking on the plus sign. Branches that have a minus sign (-) next to them can be collapsed by clicking on the minus sign.

Click on a branch to display the settings associated with it. You can change the settings by changing the selections displayed on the right hand side of the settings window. Note that some of the settings do not take effect until you save the settings and then open a new terminal or file transfer window, or start a new connection.

2.1 Saving Settings

When you have made changes to the settings, an asterisk (*) is displayed on the SSH Secure Shell client title bar, after the name of the current settings file (for example: `default*`). This indicates that the changed settings are not yet permanent - they have not been saved yet.

If you want to make the changes permanent, you can save them for later use. Click the **Save** button on the toolbar, or select the **Save Settings** option from the **File** menu to save any changes you have made to your current settings. The changes will be saved in the default settings file, `default.ssh2`.

 © 2002 SSH Communications Security Corp.

The default settings file is loaded automatically when you start the SSH Secure Shell client. Therefore all the settings that you save in the default settings file take effect immediately when you launch the Secure Shell client. These settings are also used for connections started with the **Quick Connect** option (see section 3.1 (Quick Connect)).

The positions of the currently open terminal and File Transfer windows can be saved separately with the **Save Layout** option of the **File** menu. If you arrange your window positions to suit your own taste and save the layout settings in the default settings file, the windows will be automatically positioned the way you prefer them when you next run the SSH Secure Shell client.

Note that by default all of the windows will be opened at once. This can be changed on the **Appearance** page of the **Settings** dialog so that the previously positioned windows are opened on demand when you open new terminal and File Transfer windows - see section 2.4.1 (Appearance).

If you spend a lot of effort customizing your own settings, it is a good idea to create backup copies of your customized settings files (`*.ssh2`) and store them in a safe location. This way you will not have to create the custom settings again, if your settings files are later lost for some reason (such as a hardware failure).

2.1.1 Multiple Settings Files

You can save separate settings files for each remote host computer. This can be done by using the **Profiles** option. For more information on using profiles, see section 3.2 (Profiles).

2.2 Loading Settings

It is easy to take into use a profile that has been previously saved. Select the **Profiles** option (from the **Profiles** toolbar or the **File** menu), and you will see a menu of previously saved profiles. Click on a profile, and a connection using the profile settings will immediately be started.

Note that this also works when you are already connected to a remote host computer. The profile will start a new, separate connection.

Another way to load the settings for a particular connection is to double-click the settings file name, for example in *Windows Explorer*. When the SSH Secure Shell client is installed, files with the extension .ssh2 are associated with the SSH Secure Shell client. This means that you can start the SSH Secure Shell client with any settings file loaded by just doubleclicking on that settings file.

If you regularly connect to several remote host computers, you can create shortcuts to the corresponding settings files for example on the Windows desktop. This way you can quickly open the desired connection with the relevant settings already defined, just by clicking on an icon on the desktop.

2.3 Profile Settings

With the **Profile Settings** page of the **Settings** dialog you can configure separate connection settings for each particular remote host computer. To display the profile settings, open the **Settings** dialog and click on the **Profile Settings** text on the left hand side of the dialog.

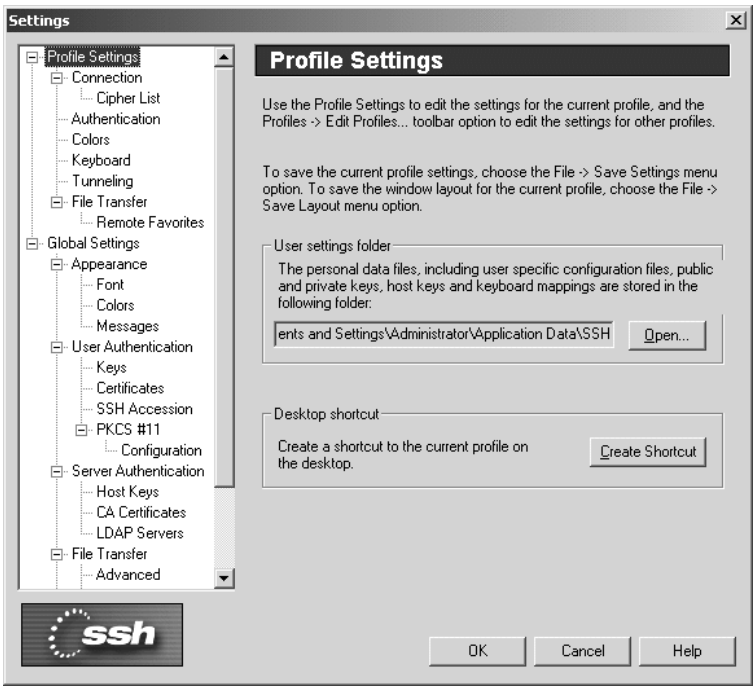

Figure 2.1: The Profile Settings page of the Settings dialog.

User Settings Folder

The directory path to your personal data files is displayed in the text field next to the **Open** button. Note that this is not an editable field, but the location of these files can be set by defining the `SSHCLIENT_USERPROFILE` environment variable. For more information, see the SSH Secure Shell FAQ (`http://www.ssh.com/faq/`).

Your personal files include the settings file (default name default.ssh2), your public and private keys, host keys and the keyboard mapping file (for example `yourmapfile.sshmap`).

Click the **Open** button to quickly access your personal data files. The folder where the settings files are saved will open. This is useful if you wish to copy or backup your personal settings.

Note that your private keys should always be kept secret. This is important to remember if you are sharing your local computer with other users. In such case, it is not advisable to store your private keys on the local disk. For more information on user key files, see section 3.6 (Using Public-Key Authentication).

Desktop Shortcut

Click the **Create Shortcut** button to create a shortcut to the currently defined profile on the Windows desktop. The shortcut will be have the name of the current profile (typically the remote host computer

 © 2002 SSH Communications Security Corp.

that you are connected to). When you later click on the shortcut, SSH Secure Shell will be launched with the settings that have been saved for the profile.

OK

Click the **OK** button to start using the specified settings.

Cancel

Click the **Cancel** button to abort any changes you have made to the settings.

Help

Click the **Help** button to see the relevant help section.

2.3.1 Connection

The protocol settings used in the connection are configured using the **Connection** page of the **Settings** dialog. Any changed connection settings will take effect the next time you login.

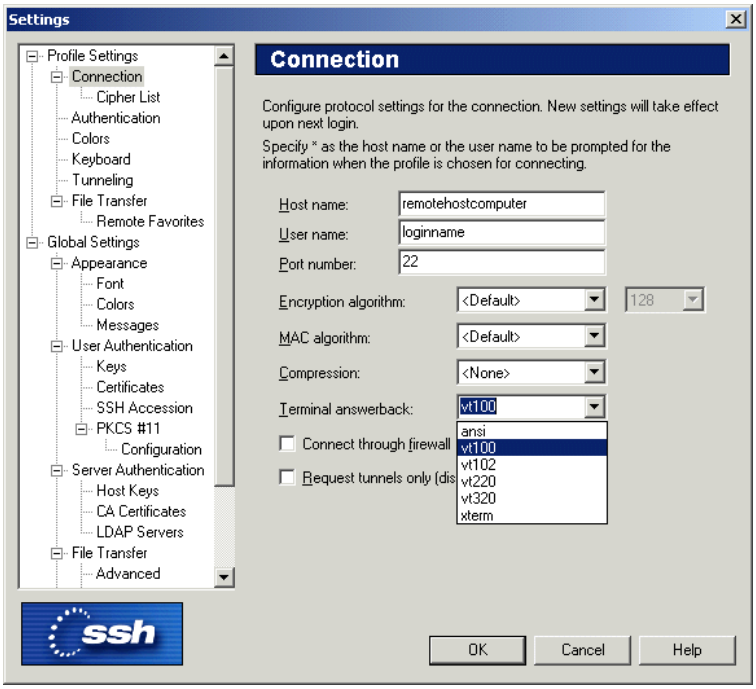

Figure 2.2: The Connection page of the Settings dialog.

Host Name

Type the name of the remote host computer which you will connect to using this profile. If you specify * (an asterisk) as the host name, you will be prompted to type in the host name when connecting.

User Name

Type the user name you want to use when connecting to the remote host computer. If you specify * (an asterisk) as the user name, you will be prompted to type in the user name when connecting.

Port Number

Type the port number you want to use for the SSH2 connection. The default port is 22.

Note: that an `sshd2` daemon program must be listening on the specified port on the remote host computer or the connection attempt will not succeed. If you are unsure of which port the remote host computer is listening to, contact the system administrator of the remote host.

Encryption Algorithm

Select the desired encryption algorithm from the dropdown menu. Valid choices are `3DES`, `Blowfish`, `Twofish`, `AES`, `Arcfour`, and `CAST`. Also DES is supported for compatibility reasons, however it is no longer considered cryptographically secure. You can also select whatever `default` that is used by the remote host computer, use no enryption (`none`) at all, or create your own customized `cipher list`. For more information on the `Cipher List` option, see section 2.3.2 (Cipher List).

For the AES and Twofish algorithms you can also choose the strength of encryption, ie. how many bits will be used. Greater values are more secure, but slower to use. Possible values are 128, 192 or 256 bits.

Note: If you select `none` as the encryption algorithm, the communications for this profile will not be encrypted and all information will be sent as plaintext. The `none` encryption method is not secure and its use is not recommended. Use it only if you are sure of what you are doing. If you select this option, a warning dialog will be displayed.

MAC Algorithm

Select the desired Message Authentication Code (MAC) algorithm (hash algorithm) from the dropdown menu. Valid choices are `HMAC-MD5` and `HMAC-SHA1`. You can also select whatever `default` that is used by the remote host computer, or select to use no message authentication code at all (`none`). If you select not to use any MAC algorithm, a confirmation dialog will be displayed.

Compression

Select the desired compression setting from the dropdown menu. Valid choices are `zlib` and `none`. Compression is disabled by default.

Terminal Answerback

Select the desired terminal answerback from the dropdown menu. Possible choices are `ansi`, `vt100`, `vt102`, `vt220`, `vt320` and `xterm`.

Connect through Firewall

Select the checkbox if you are connecting through a firewall. For more information on the firewall settings, see section 2.4.21 (Firewall).

Request Tunnels Only (Disable Terminal)

Select the **Request Tunnels Only** checkbox if you wish to only set up the specified tunnels and not request a terminal or file transfer session.

 © 2002 SSH Communications Security Corp.

2.3.2 Cipher List

With the **Cipher List** page of the **Settings** dialog you can control which ciphers can be used for the connection. This selection defines what encryption methods will be available when using the `Cipher List` encryption algorithm setting.

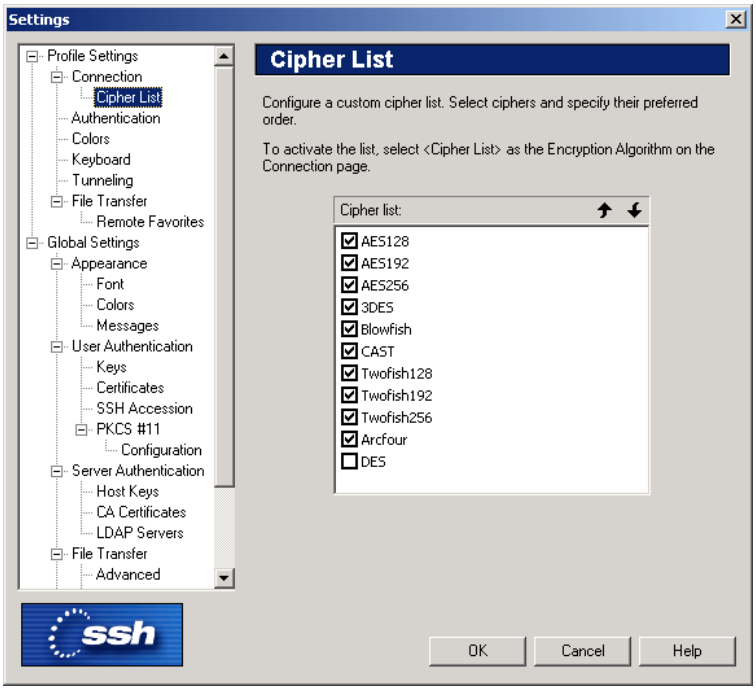

Figure 2.3: Select your preferred encryption algorithms with the Cipher List page.

The following algorithms can be selected:

AES128

AES192

AES256

3DES

Blowfish

CAST

Twofish128

Twofish192

Twofish256

Arcfour

DES

DES is a legacy cipher that is not considered to be cryptographically secure. DES is only included for compatibility with some older protocol versions. It is *strongly* recommended that DES is not used.

You can change the ciphers' order of preference with the **Up** and **Down** buttons.

Up

You can give a cipher a higher priority by clicking it with the mouse, and then clicking the **Up** button. The marked algorithms that are located on the top of the list are preferred.

SSH Secure Shell will try to use the first marked algorithm in the connection. If that algorithm is not supported by the remote host computer, the client software will try the next marked algorithm on the list, and so on.

Down

To give a cipher a lower priority rating, select it with the mouse, and then click the **Down** button.

Select the checkbox next to each algorithm to include or exclude it in the list of available custom algorithms. An algorithm marked with a check mark is available for use.

To use your customized list of preferred encryption algorithms, select `Cipher List` as the encryption algorithm on the **Connection** page of the **Settings** dialog. For more information, see section 2.3.1 (Connection).

2.3.3 Authentication

With the **Authentication** page of the **Settings** dialog, you can define customized authentication methods. Two lists are displayed on the page, the upper list for general authentication, and the lower list for authentication methods user for public-key authentication.

The icons displayed above the list can be used to add a new authentication method, delete an existing authentication method and move the authentication methods upwards or downwards in the preference list. Authentication methods higher up in the list will be attempted first. Usually authentication methods that require user interaction should be attempted last.

Authentication Methods

Possible methods for general authentication are the following:

Public Key

Use public-key authentication.

Password

Use password for authentication.

 © 2002 SSH Communications Security Corp.

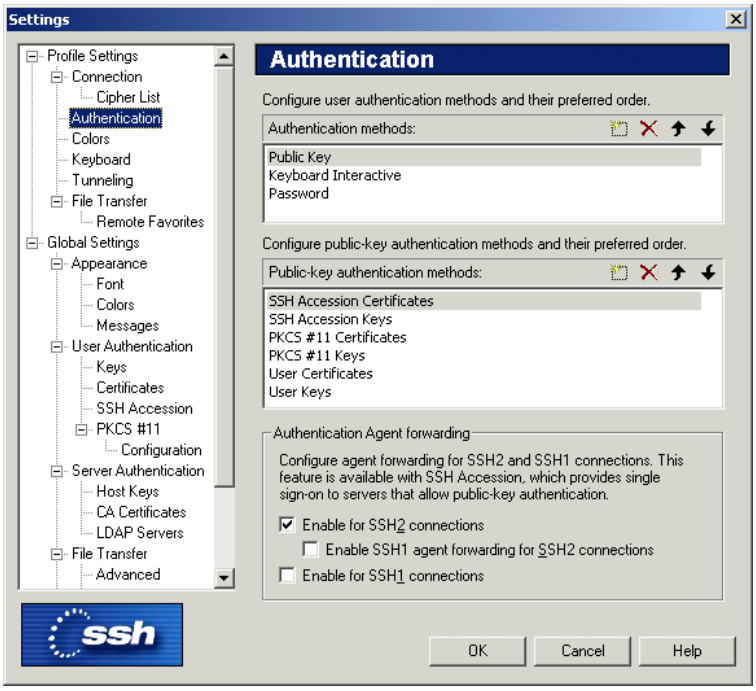

Figure 2.4: Defining the authentication settings

Keyboard-Interactive

Keyboard-Interactive is designed to allow the Secure Shell client to support several different types of authentication methods. For more information on Keyboard-Interactive, see Section 8.4 (Keyboard-Interactive Authentication).

SecurID

Using SecurID authentication requires that you have a SecurID device that generates the numeric codes that are needed to login.

PAM

Use Pluggable Authentication Modules (PAM) for authentication. PAM is an authentication method that has gained wide popularity especially on UNIX platforms.

The default authentication methods are public-key authentication, Keyboard-Interactive and password authentication.

Public-Key Authentication Methods

Possible methods for public-key authentication are the following:

SSH Accession Certificates

Use SSH Accession for authentication. *SSH Accession* is a separate software product by SSH Communications Security that offers an easy method for accessing authentication credentials on smart cards and other hardware tokens. It can be also used as an authentication agent. For more information, see `http://www.ssh.com/products/accession/`.

SSH Accession Keys

Use SSH Accession keys for authentication. *SSH Accession* is a separate software product by SSH Communications Security that offers an easy method for accessing authentication credentials on smart cards and other hardware tokens. It can be also used as an authentication agent. For more information, see `http://www.ssh.com/products/accession/`.

PKCS #11 Certificates

Authenticate by using PKCS #11 certificates (certificates stored for example on a smart card or a USB token). For more information on using PKCS #11 certificates, see section 2.4.10 (PKCS 11).

PKCS #11 Keys

Authenticate by using PKCS #11 keys (keys stored for example on a smart card or a USB token). For more information on using PKCS #11 keys, see section 2.4.10 (PKCS 11).

User Certificates

Use user certificates for authentication. For more information on using certificates, see section 2.4.7 (Certificates).

User Keys

Use user keys for authentication. For more information on using user keys, see section 2.4.6 (User Keys).

Note: The automatically handled authentication methods should always be listed first, i.e. public-key authentication should preceed password authentication. This way the automatically handled method will be used whenever possible.

Authentication Agent Forwarding

Authentication agent is a program to automatize the use of authentication private keys. *SSH Accession* can provide agent functionality for SSH Secure Shell Windows client.

When you use the agent, it will be automatically used for public-key authentication. This way, you only have to type the passphrase of your private key once to the agent. Furthermore, authentication data does not have to be stored on any other machine than the local machine, and authentication passphrases or private keys never go over the network.

Agent forwarding can be enabled or disabled based on the Secure Shell protocol used. Select the checkbox for any of the options you want to use:

 © 2002 SSH Communications Security Corp.

Enable SSH2 connections

Select this checkbox to allow authentication agent forwarding to be used for connections using the SSH protocol version 2.

Enable SSH1 agent forwarding for SSH2 connections

Select this checkbox to allow authentication agent forwarding with the SSH protocol version 1 to be used for connections that use the SSH protocol version 2.

Enable for SSH1 connections

Select this checkbox to allow authentication agent forwarding to be used for connections using the SSH protocol version 1.

2.3.4 Colors

The colors used in the terminal window can be selected using the **Colors** page of the **Settings** dialog. The new color settings are active immediately when you click the OK button.

You can select from the following 16 colors: black, maroon, green, olive, navy, purple, teal, silver, gray, red, lime, yellow, blue, fuchsia, aqua and white.

Note that changing the terminal colors does not affect what is already visible on the terminal window, but the text output from this point onwards will use the set color scheme.

To discard your changes, click the **Cancel** button.

Use Global Colors

Select the **Use Global Colors** checkbox if you want to use the same color settings for each connection. If the checkbox is selected, you cannot specify different color settings for each connection profile (the other color settings are grayed out).

The **Use Global Colors** checkbox is visible only on the **Colors** page that is located under Profile Settings in the **Settings** dialog.

Text Colors

The text colors affect the terminal window background color and the color of text in both a connected window and a disconnected window.

Foreground

Select the desired foreground color from the dropdown menu. Foreground color is used for text in a window that has a connection to a remote host computer. Sixteen colors are available for your selection. Black is the default foreground color.

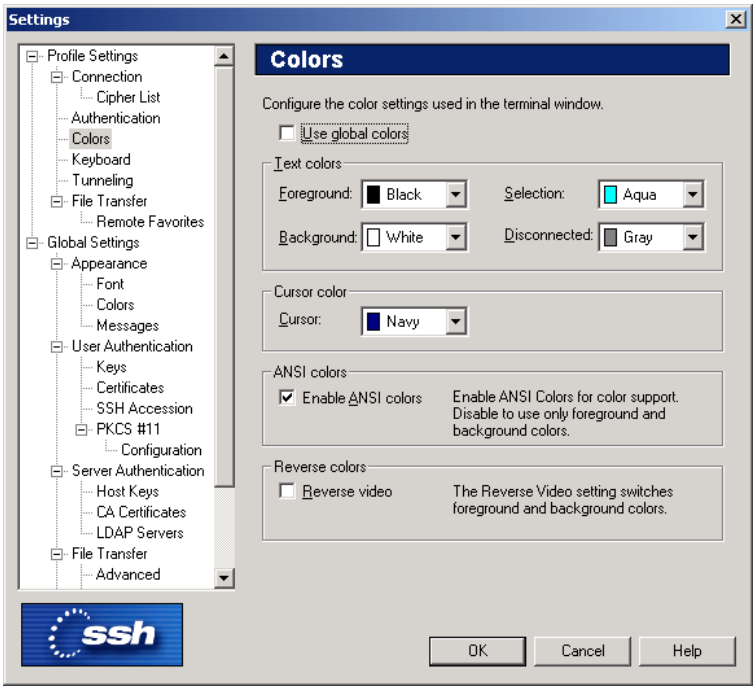

Figure 2.5: The Colors page of the Settings dialog.

Background

Select the desired background color from the dropdown menu. Sixteen colors are available for your selection. White is the default background color.

Selection

Use the dropdown menu to select the color that will be used as the background color when selecting text with the mouse. Sixteen colors are available for your selection. Aqua is the default selection color.

Disconnected

Use the dropdown menu to select the color that will be used as the foreground color in a terminal window that has no connection to a remote host computer. Sixteen colors are available for your selection. Gray is the default foreground color for a disconnected terminal window.

Cursor Color

Select the desired cursor color from the dropdown menu. Sixteen colors are available for your selection. Navy is the default cursor color.

ANSI Colors

With ANSI control codes it is possible to change the color of text in a terminal window. With the ANSI Colors setting you can select if you want to allow this feature or not. Even if you disable ANSI colors, you

can still select your favorite text and background colors to be used in the terminal window.

Enable ANSI Colors

Select the Enable ANSI Colors checkbox to allow ANSI colors to be used in the terminal window. By default, ANSI colors are on.

Reverse Colors

By reversing the display colors you can quickly change the display from positive (dark on light) to negative (light on dark) to improve visibility.

Reverse Video

Select the Reverse Video checkbox to change the foreground color into background color and vice versa. This setting affects the whole terminal window as soon as you click the OK button.

2.3.5 Keyboard

The keyboard settings used for the connection are configured using the **Keyboard** page of the **Settings** dialog. Keyboard mappings take effect when you start a new connection or reset the terminal.

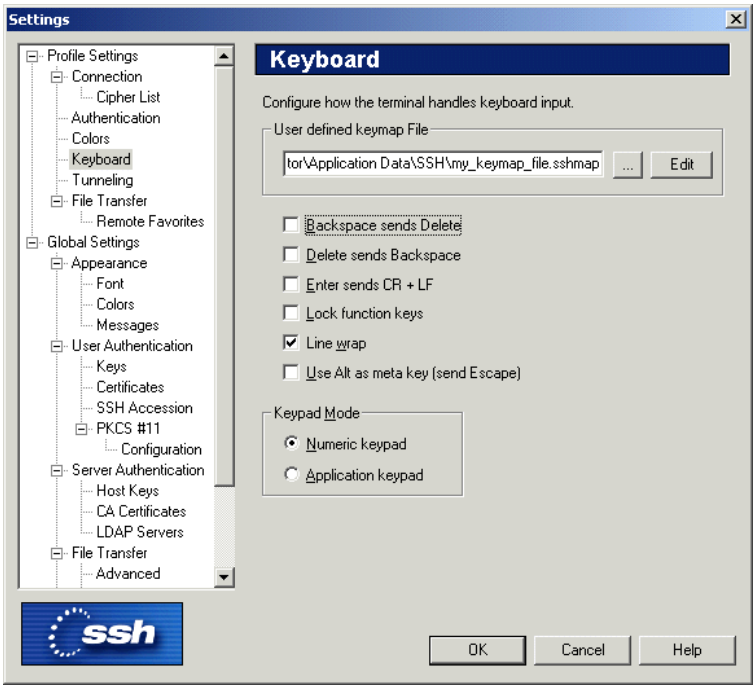

Figure 2.6: The Keyboard page of the Settings dialog.

User Defined Keymap File

With the **User Defined Keymap File** option you can create additional keyboard shortcuts or modify the existing ones. The additional key mappings are saved into a separate file with the `.sshmap` file extension. The current keymap file is displayed on the text field.

You can customize the current key mappings by clicking the **Edit** button. The Keymap Editor dialog will appear. For more information on using the Keymap Editor, see section 2.3.6 (Keymap Editor).

If you have an alternative keymap settings file already defined, you can load it by typing the path and file name in the text field, or by clicking on the button on the righthand side of the text field. Clicking the button will open an Open dialog that allows you to locate an alternative keymap file.

Backspace sends Delete

Select the **Backspace sends Delete** checkbox if you want to map the Backspace key to the Delete operation.

Delete Sends Backspace

Select the **Delete Sends Backspace** checkbox if you want to map the Delete key to the Backspace operation.

Enter sends CR + LF

Select the **Enter sends CR + LF** checkbox if you want to map the Enter key to send the carriage return (CR) and line feed (LF) characters. Otherwise only the line feed character will be sent.

Lock Function Keys

Select the **Lock Function Keys** checkbox if you want to lock the function keys.

Line Wrap

Select the **Line Wrap** checkbox if you want the text lines to wrap on the terminal window's edge. By default, line wrapping is on.

Use Alt as meta key (send Escape)

Select the **Use Alt as meta key (send Escape)** checkbox if you want the `Alt` key to function as the meta key in the same way as the `Escape` key. If this option is selected, you can for example press the `Alt+X` key combination to simulate the `Escape` followed by `X`.

Keypad Mode

Select how you want the numeric keypad on the right hand side of the regular keyboard to function.

Numeric Keypad: The keypad is used to type numbers.

Application Keypad: The keypad is used for application control (with the keypad keys functioning as cursor keys, `Home`, `End`, `Page Up`, `Page Down`, `Insert` and `Delete`).

2.3.6 Keymap Editor

The **Keymap Editor** dialog displays any customizations made to the current keymap. Using the editor you can define additional key mappings, open saved keymap files and create new keymap files.

 © 2002 SSH Communications Security Corp.

Figure 2.7: Customizing the keymap

The icons on the top of the Keymap Editor dialog allow you to start a new keymap file from scratch, to open an already defined keymap file, or to save the current keymap customizations into a keymap file:

New

Click the **New** button to start creating a new keymap file. This will clear all the current keymap customizations.

Open

Click the **Open** button to load an already defined keymap file for further customization. The Open dialog will appear, allowing you to locate the desired keymap file.

Save

Click the **Save** button to save the current keymap customizations to the currently open keymap file. If no keymap file has been loaded, the Save As dialog will open, allowing you to specify the file name for a new keymap file.

Save As

Click the **Save As** button to save the current keymap customizations into a different keymap file. The Save As dialog will open, allowing you to specify the file name for a new keymap file.

The large area in the center of the Keymap Editor dialog displays the defined keymap customizations. The **Key** column on the left displays the key combination whose function has been customized and the Function column displays the effect that pressing this particular key combination will cause.

The buttons on the bottom of the Keymap Editor dialog allow you to customize the keymap settings of the current keymap file:

Add

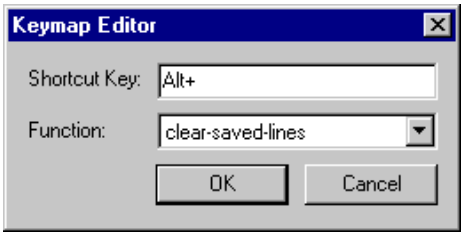

Figure 2.8: Modifying a keymap customization

Click the **Add** button to add a new keymap customization. A small **Keymap Editor** dialog appears. Place the cursor on the **Shortcut Key** line and press a key combination on the keyboard to select which key binding you want to modify. The select the desired function for that keypress from the Function drop-down menu.

Edit

Select an already defined keymap customization and click the **Edit** button to modify the selected customization.

Remove

Select an already defined keymap customization and click the **Remove** button to delete the selected customization.

Exit

Click the **Exit** button to close the Keymap Editor dialog. If you have not saved all your keymap customizations, a Confirm dialog will open, asking if you want to save the changes you have made or cancel the exit operation.

2.3.7 Tunneling

Tunneling, or port forwarding, is a way to forward otherwise insecure TCP traffic through encrypted SSH Secure Shell tunnel. You can secure for example POP3, SMTP and HTTP connections that would otherwise be insecure.

Note: The client-server applications using the tunnel will carry out their own authentication procedures (if any) the same way they would without the encrypted tunnel.

Tunneling settings are configured using the **Tunneling** page of the **Settings** dialog. Any changed tunneling settings will take effect the next time you login.

The outgoing and incoming tunnel settings are configured using the **Outgoing** and **Incoming** tabs of the **Tunneling** page.

 © 2002 SSH Communications Security Corp.

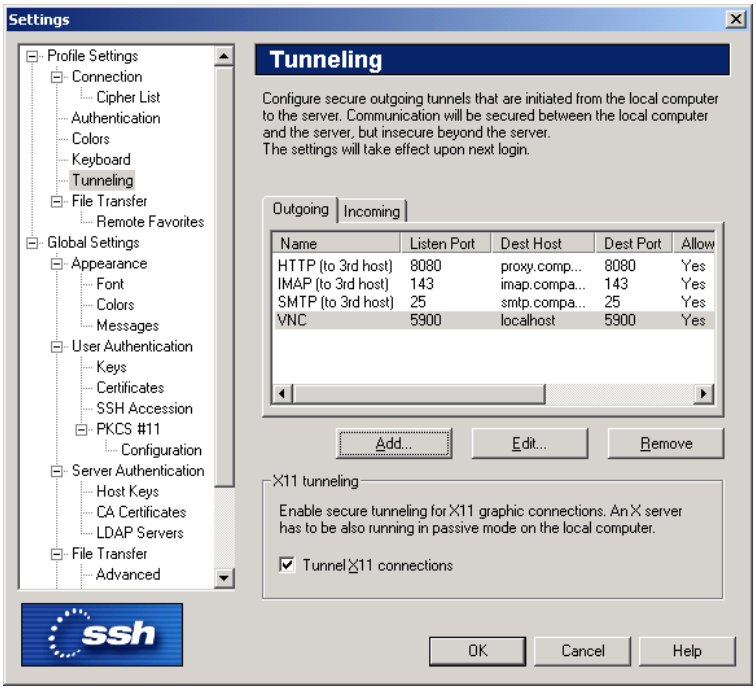

Figure 2.9: The Tunneling page of the Settings dialog.

Outgoing

Outgoing tunnels protect TCP connections that your local computer forwards from a specified local port to the specified port on the remote host computer you are connected to.

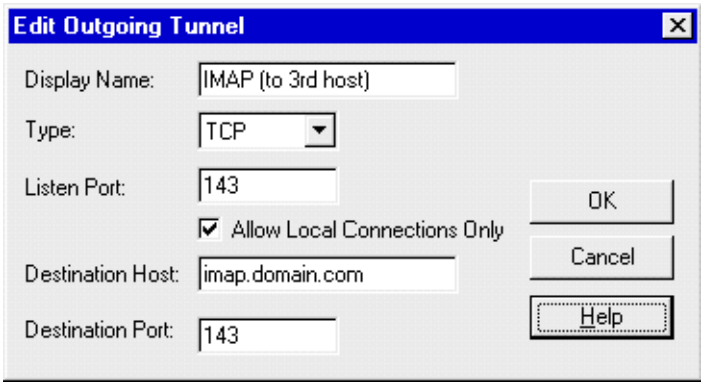

Figure 2.10: Tunneling an IMAP connection for secure email.

It is also possible to forward the connection beyond the remote host computer, however the connection is encrypted only between the client (local computer) and the Secure Shell server. See 2.11 (Forwarding to a third host).

Click the **Outgoing** tab to edit outgoing tunnel definitions.

Figure 2.11: Forwarding to a third host.

The following fields are used to define an outgoing tunnel. These values can be edited by clicking the Add or Edit buttons on the Outgoing page of the Settings dialog.

Name

The name of the tunnel definition. You can use this field to type in a descriptive name that will help you to recognize this tunnel definition later on.

Listen Port

This is the number of the local port that the tunnel 'listens to', or captures.

Note: The protocol or application that you wish to create the tunnel for may have a fixed port number (for example, 143 for IMAP) that it needs to use to successfully connect. Some other protocol or applications may require an offset (e.g. 5900 for VNC) that you will have to take into an account.

Destination Host

This field defines the destination host for the port forwarding. The default value is `localhost`.

Note: The value of `localhost` is resolved after the Secure Shell connection has been established - so here `localhost` refers to the remote host computer you have connected to.

Destination Port

The destination port defines what port will be used for the forwarded connection on the destination host.

Allow Local Connections Only

Leave a check mark in this box if you allow only local connections to be made. This means that other computers will not be able to use the tunnel created by you. By default, only local connections are allowed. This is the right choice for most situations. You should carefully consider the security implications if you decide to also allow outside connections.

Type

Select the type of the tunnel from the dropdown list. Valid choices are TCP and FTP.

Incoming

Incoming tunnels protect TCP connections that the remote host forwards from a specified remote port to the specified port on your local computer. Click the **Incoming** tab to edit incoming tunnel definitions.

 © 2002 SSH Communications Security Corp.

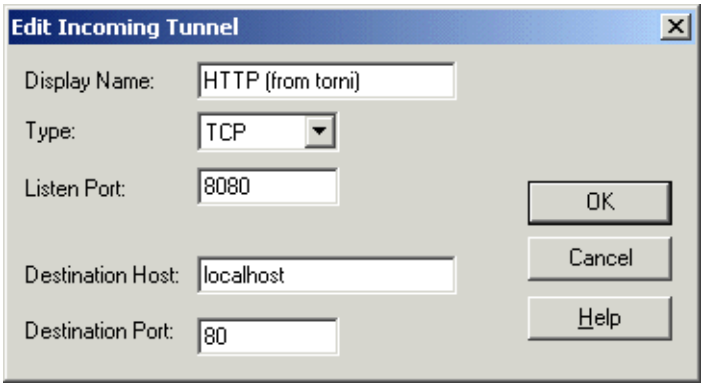

Figure 2.12: Redirecting the HTTP connection to a remote host port 8080 to your local computer's port 80.

The following fields are used to define an incoming tunnel. These values can be edited by clicking the Add or Edit buttons.

Name

The name of the tunnel definition. You can use this field to type in a descriptive name that will help you to recognize this tunnel definition later on.

Listen Port

The port that the tunnel 'listens to', or captures from the remote host computer.

Note: Privileged ports (above 1023) can be forwarded only when logging in with root privileges on the remote host computer.

Destination Host

This field defines the destination host for the port forwarding. The default value is `localhost`.

Note: Here `localhost` refers to your local computer. Also note that if the connection from the remote host computer is forwarded beyond your local computer, that connection will be insecure.

Destination Port

The destination port defines what port will be used for the forwarded connection on the destination host.

Type

Select the type of the tunnel from the dropdown list. Valid choices are TCP and FTP.

Configuring Tunnels

The following buttons are available for configuring outgoing and incoming tunnels.

Add

Click the **Add** button to add a tunnel definition. An **Add New Tunnel** dialog appears, allowing you to define the name, type, listen port, destination host, and destination port for the port forwarding. With outgoing tunnels you can also define if you allow local connections only.

Note: If you are tunneling an FTP connection, you must set the tunnel type as FTP.

If the SSH server and the FTP server are located on separate host computers, FTP tunneling works only if FTP is set to run in passive mode. If the SSH server and the FTP server are located on the same computer, tunneling works regardless of whether FTP is running in passive or active mode.

Edit

Select a tunnel definition from the displayed list and click the Edit button to edit a previously defined tunnel. An Edit Tunnel dialog appears, allowing you to edit the name, listen port, destination host, and destination port of the outgoing tunnel. With outgoing tunnels you can also define if you allow local connections only.

Remove

Select a tunnel definition from the displayed list and click the **Remove** button to remove a previously defined tunnel. Note that the selected tunnel will be removed immediately, with no confirmation dialog being displayed.

X11 Tunneling

The Secure Shell 2 client can securely tunnel (forward) X11 graphic connections from the remote host computer to an X- Windows server running on the local computer.

Note: You must also be running an X emulator such as *Exceed* or *Reflection X* in passive mode on the Windows computer for X11 tunneling to work.

To tunnel (forward) X11 traffic, perform the following tasks:

1. Install an X server (X emulation) program on Windows (*eXceed*, *Reflection X*, or the like).
2. Start the SSH Secure Shell for Workstations Windows client.
3. Select the **Edit -> Settings... -> Tunneling** option and make sure that the **Tunnel X11 connections** checkbox is selected.
4. Save your settings for SSH Secure Shell for Workstations Windows client.
5. Quit the Windows client, start it again and log into the remote host.
6. Start the X server (X emulation) program.
7. Run `xterm` or `xclock` from SSH Secure Shell, and it should work.

 © 2002 SSH Communications Security Corp.

2.3.8 File Transfer

The profile-specific file transfer settings can be configured using the **File Transfer** page located on the **Profile Settings** branch of the **Settings** dialog. The new settings will affect subsequently started File Transfer windows.

The profile-specific file transfer settings affect how ASCII (plain text) files are handled. On Windows systems, a line break is specified by using two special characters, Carriage Return and Linefeed (CRLF, with ASCII values of 13 and 10). Unix systems use only Linefeed (LF, or the ASCII value 10) for this purpose.

When the correct ASCII transfer settings are specified, SSH Secure Shell will perform the required line break conversion automatically.

Note: If you are connecting to an SSH Secure Shell version 3.2 server (or newer), the host type does not need to be configured. If the server version is older or produced by some other vendor, the host type may need to be specified.

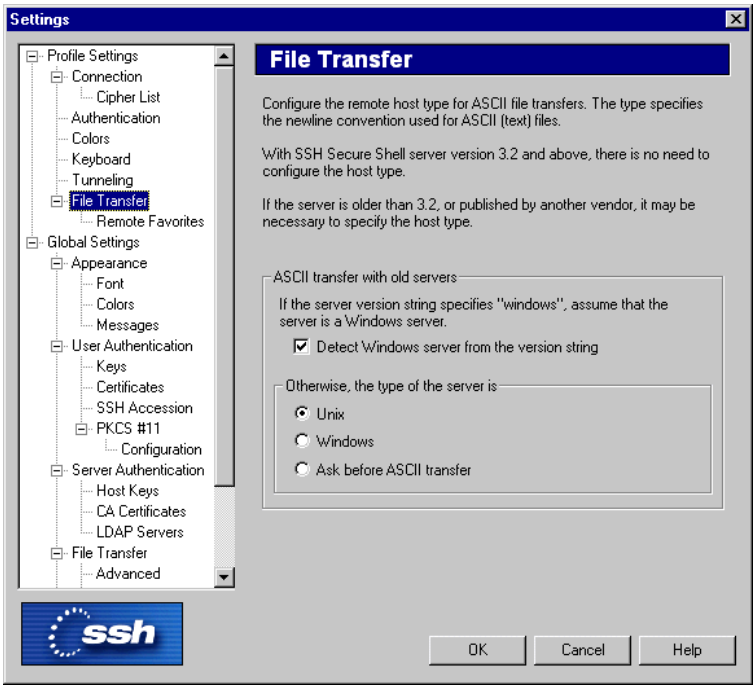

Figure 2.13: The profile-specific File Transfer page of the Settings dialog.

ASCII transfer with old servers

Detect Windows server from the version string

Select this checkbox to automatically detect Windows servers and use the correct setting for them. For this feature to work correctly, the Windows server has to specify ”windows” in its version string.

Unix

Select the Unix checkbox to use Unix compatible line breaks (LF).

Windows

Select the Windows checkbox to use Windows compatible line breaks (CRLF).

Ask before ASCII transfer

If you select this checkbox, the SSH Secure Shell client will ask you to specify the server type before each ASCII file transfer.

2.3.9 Favorites

On the **Favorites** page of the **Settings** dialog you can create a list of commonly used directories. These favorites can then be easily selected from a drop-down menu in the File Transfer window.

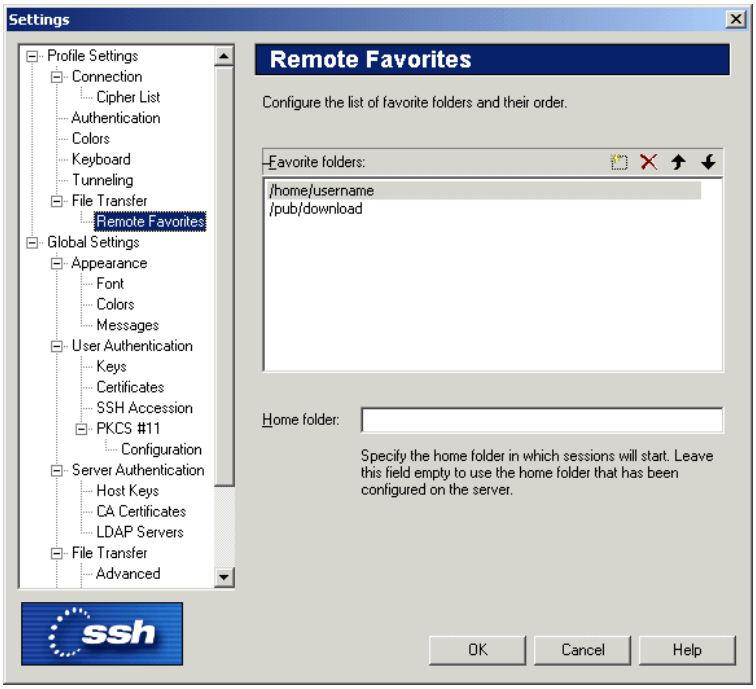

Figure 2.14: Creating a list of most commonly used directories.

Favorite Folders

This list contains the favorite folders you have defined for the current connection profile. You can add, remove and sort the favorites by using the icons displayed above the list:

New

Click the **New** button to add a new favorite, and then type the path to the desired folder.

 © 2002 SSH Communications Security Corp.

Delete

Select an already defined favorite from the list and then click the **Delete** button to remove it from the list.

Up

Select an already defined favorite from the list and then click the **Up** button to move it higher in the list.

Down

Select an already defined favorite from the list and then click the **Down** button to move it lower in the list.

Home Folder

In the **Home Folder** field you can type the directory where any new connections associated with this profile will start. If you leave the field empty, new connections will use the remote home folder that has been specified for your user account on the remote host computer.

2.4 Global Settings

Global configuration settings are configured using the **Global Settings** page of the **Settings** dialog. Global settings are common for all connections to remote host computers.

Global settings are saved at the same time as profile settings. Global settings are always saved in the user profile directory with the filename `global.dat`.

2.4.1 Appearance

The appearance of the application and the terminal window is configured using the **Appearance** page of the **Settings** dialog.

Office XP Look

Select the **Office XP Look** check box to change the way the menu bar and tool bar are displayed to match the visual style of Microsoft Office XP.

Show the Add Profile Dialog when connected using Quick Connect

Select the **Show the Add Profile Dialog when connected using Quick Connect** check box to briefly display the Add Profile dialog when connecting to a remote host computer using Quick Connect. This allows you to create a profile for the host simply by typing in the profile name.

Figure 2.15: The Global Settings page of the Settings dialog.

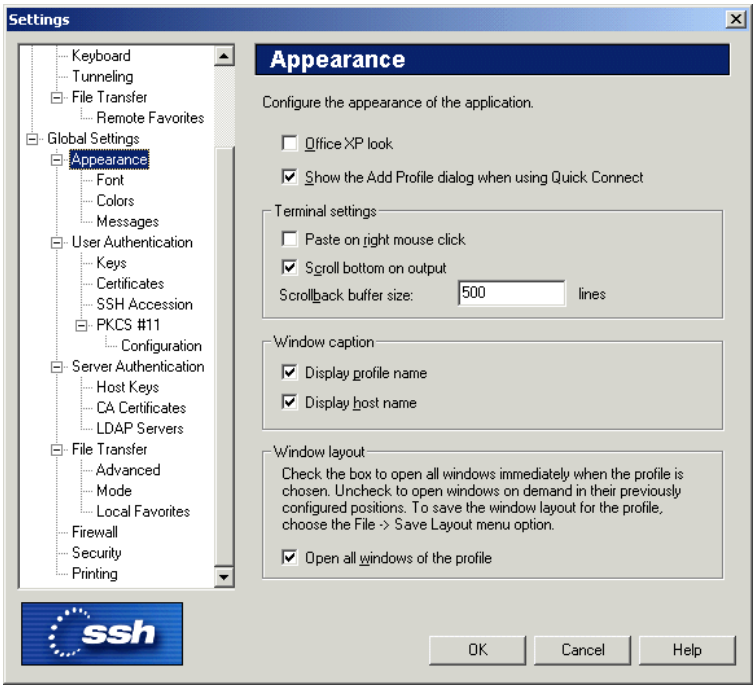

Figure 2.16: The Appearance page of the Settings dialog.

Terminal Settings

With the Terminal Settings options you can define how the terminal window works.

Paste on Right Mouse Click

Select the **Paste Selection on Right Mouse Click** check box to enable fast copying of text on the terminal display. When you have this option selected, you can copy text simply by highlighting it and then paste it by clicking the right mouse button.

Scroll Bottom on Output

Select the **Scroll Bottom on Output** checkbox to have the terminal window scroll to the bottom whenever new text is output. If this option is not selected, you can view the terminal window without the windows scrolling to the bottom every time a new line of text is displayed. By default, this option is on.

Scrollback Buffer Size

Type in the **Terminal Scrollback Size** field the number of lines that you want to collect in the scrollback buffer. The larger the value, the more you can scroll back the terminal display to view previous terminal output. The default value is 500 lines.

Window Caption

The **Window Caption** settings affect what is displayed in the title bar of the SSH Secure Shell for Workstations Windows client terminal window and the File Transfer window.

Display Profile Name

Select the **Display Profile Name** check box to have the name of the current profile to be displayed on the title bar.

Display Host Name

Select the **Display Host Name** check box to have the host name of the currently connected remote host computer to be displayed on the title bar.

Window Layout

If you have created a connection profile with several windows open at the same time and saved the layout, all of the windows associated with the profile are normally opened when you select the profile. With the Window Layout option you can override this behavior.

Open all windows of the profile

Select the **Open all windows in the profile** check box to open all the windows associated with a profile when the profile is selected. If this option is not selected, the other windows open in their configured positions when you open new windows. By default, this option is on.

2.4.2 Font

The font used in the terminal window can be selected using the **Font** page of the **Settings** dialog. The new font setting affects the terminal window immediately when you click the **OK** button. To discard the changes, click the **Cancel** button.

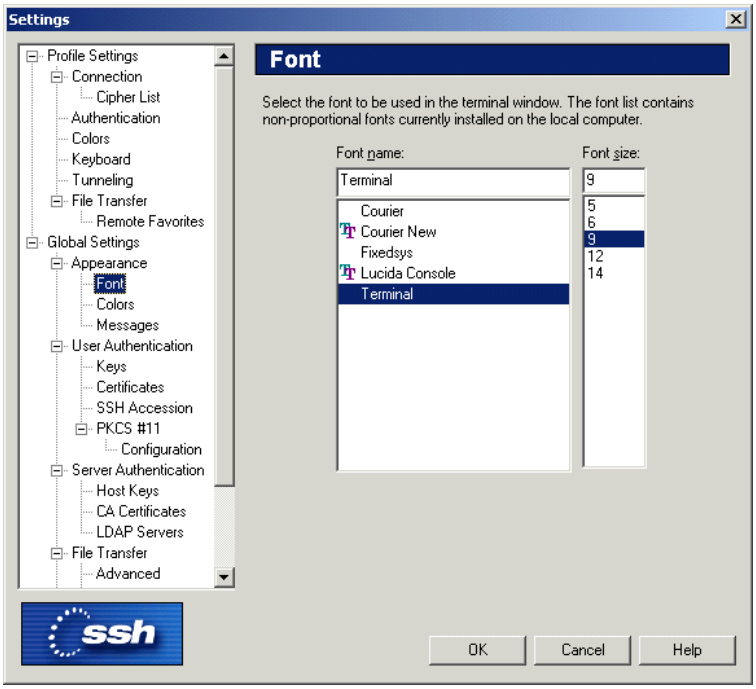

Figure 2.17: The Font page of the Settings dialog.

Font Name

Select the desired font from the **Font Name** list. The list displays the non-proportional (fixed-width) fonts installed in your local computer. Note that proportional fonts are not suitable for the terminal window and therefore are not available for selection.

Font Size

Select the desired font size from the **Font Size** list. Note that the font size affects the size of the terminal window: the smaller font you select, the smaller the terminal window will be, and vice versa. However, after this operation the size of the terminal window can be modified to suit your tastes.

2.4.3 Colors

The color settings can be defined either globally or per profile. When the colors are defined under the Global Settings display, the **Use Global Colors** option is not available, but the color settings will affect all connection profiles.

For more information, see section 2.3.4 (Colors).

 © 2002 SSH Communications Security Corp.

2.4.4 Messages

On the **Messages** page of the **Settings** dialog you can configure default replies to standard messages that normally ask for user confirmation.

The messages are listed under several categories. Categories that have a plus sign (+) next to them can be expanded by clicking on the plus sign. Expanded categories have a minus sign (-) next to them and can be closed by clicking on the minus sign.

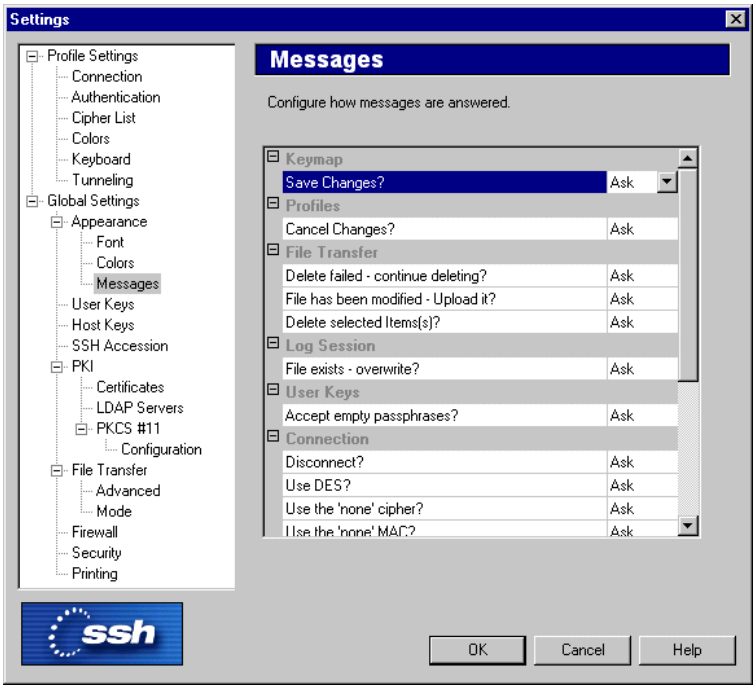

Figure 2.18: Customizing which confirmation dialogs are displayed

Each confirmation can be set to automatically accept (`Yes`) or reject (`No`) the action, or to ask the user for confirmation (`Ask`). By default all messages ask the user to confirm the action.

2.4.5 User Authentication

There are several different methods that can be used to authenticate the user when connecting to a remote host computer. In most situations, the most convenient user authentication methods are public-key authentication, certificate authentication or authentication with hardware tokens (smart cards).

To use *public-key authentication*, you must upload your public key to your home directory on the remote host computer. You also have to modify your `authorization` file to allow connection with the new key. For more information, see Section 3.5.2 (Manually Editing the Authorization File). By default, all available public keys and certificates are offered to the remote host computer during public-key authentication.

Certificate authentication is more secure than the traditional public-key authentication, as the system verifies

Settings
Profile Settings
Connection
Cipher List
Authentication
Colors
Keyboard
Tunneling
File Transfer
Remote Favorites
Global Settings
Appearance
Font
Colors
Messages
User Authentication
Keys
Certificates
SSH Accession
PKCS #11
Configuration
Server Authentication
Host Keys
CA Certificates
LDAP Servers
File Transfer
Advanced
User Authentication
The client supports several user authentication methods. The public-key authentication methods are configured on the User Authentication configuration pages. All the other methods require no additional configuration.
The attempted authentication methods for a profile can be selected on the 'Authentication' page of the Profile Settings.
The public key authentication is performed either by relying on public keys or certificates. The key pairs and certificates can be used from a local hard disk or from an external source such as a smart card.
SSH Accession Lite provides authentication agent functionality for SSH Secure Shell. Various secure hardware tokens such as smart cards and USB tokens as well as software keys are supported.
By default, all available public keys and certificates are offered to the server during public-key authentication. Certificate authentication and PKCS #11 hardware tokens are supported only in commercial distributions.
Configure the general options for hardware tokens:
Token insertion and removal
Disconnect automatically when token is removed
Connect automatically when token is reinserted
Seconds to wait before disconnecting:
0
ssh
OK
Cancel
Help

Figure 2.19: The User Authentication page of the Settings dialog.

that the user certificate has been issued by a trusted Certificate Authority (CA) and that the certificate has not been revoked. Certificate authentication is also more convenient, as no local database of user public keys is required on the remote host computer.

Probably the most convenient method is to use a hardware token (smart card) that must be inserted into a card reader device to authenticate the user.

Note: Certificate authentication and PKCS #11 hardware tokens are supported only in the commercial versions of SSH Secure Shell.

Token Insertion and Removal

The following options specify how hardware tokens are used for user authentication:

Disconnect automatically when token is removed

Select this checkbox to immediately terminate the connection if your token is removed from the card reader device. This ensures that a connection will be active only when a token is present.

Connect automatically when token is reinserted

Select this checkbox to automatically reconnect when your token is again inserted in the card reader device. This checkbox is active only if the *Disconnect automatically when token is removed* check box is selected.

 © 2002 SSH Communications Security Corp.

Seconds to wait before disconnecting

In the text field you can specify how many seconds the connection will remain open if your token is removed from the card reader device. The default value is zero. This field is active only if the *Disconnect automatically when token is removed* check box is selected.

2.4.6 Keys

Key pairs used for user public-key authentication can be managed using the **User Keys** page of the **Settings** dialog.

Before you can use public-key authentication, you must generate a key pair for yourself. Then you must upload your public key to your home directory on the remote host computer. You also have to modify your `authorization` file to allow connection with the new key. For more information, see Section 3.3 (Key Generation).

Note: Your private keys should always be kept secret. This is important to remember if you are sharing your local computer with other users. In such case, it is not advisable to store your private keys in the local disk. For more information on user key files, see section 3.6 (Using Public-Key Authentication).

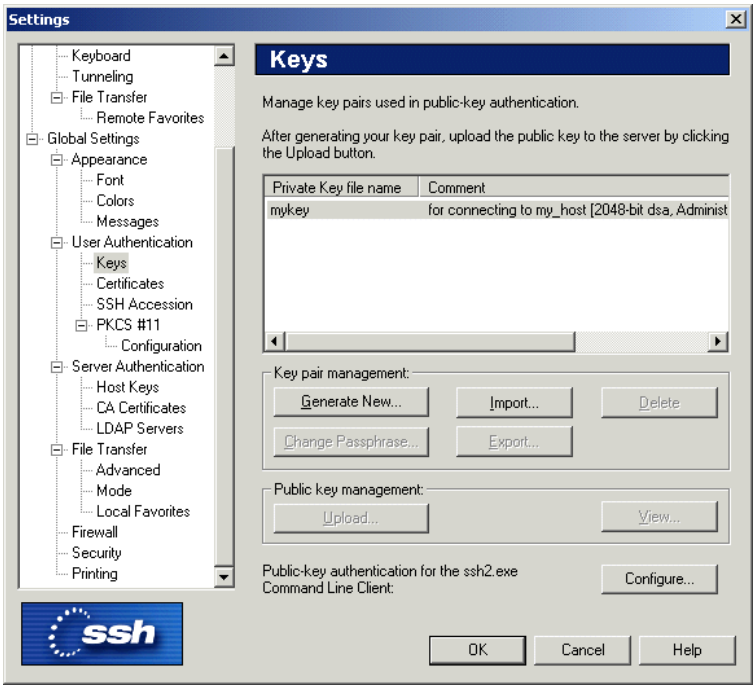

Figure 2.20: The Keys page of the Settings dialog.

Private key file list

The private key file list (located above the buttons on the **User Keys** page) shows the files used to store your private keys. The public keys are not displayed, as they have the same file names as the private keys, but with `.pub` as the file extension.

Private Key File Name

The Private Key File Name column displays the file names of your private keys.

Comment

The Comment column displays the comments (if any) associated with your private keys.

Buttons:

Below the private key list there are several buttons that can be used to administer your key files:

Generate New Keypair

Click the **Generate New Keypair** button to create a new public and private user key pair. This will bring up the **Key Generation Wizard**. For more information on this procedure, see section 3.3.1 (Key Generation Wizard).)

Delete Keypair

Select a key file from the private key file list and click the **Delete** button to delete the key file from your local computer.

Export Keypair

Select a key file from the private key file list and click the **Export Keypair** button to export the key pair. A **Select Folder** dialog will open, allowing you to specify the target location.

Import Keypair

Click the **Import Keypair** button to import a keypair. The **Import Keypair - Select Files** dialog will open, allowing you to locate the keypair to be imported.

View Public Key

Select a previously generated private key file from the private key file list and click the **View Public Key** button to display the corresponding public key. The public key file will be displayed in *Notepad*.

Change Passphrase

Select a previously generated private key file from the private key file list and click the **Change Passphrase** button to change the passphrase for the key.

Upload Public Key

Clicking the **Upload Public Key** button while connected to a remote server will automatically upload the selected public key. For more information on this procedure, see section 3.5 (Uploading Your Public Key).

 © 2002 SSH Communications Security Corp.

Configure Command Line Client ssh2.exe Keys

Click the button to write the `identification` file that is used by the command line tool `ssh2.exe` to specify which keys can be used for authentication. All the keys listed in the private key list will be included in the `identification` file. If you want to disable some keys, you can then manually delete them from the `identication` file.

The identification file will be placed in the user settings folder. The actual directory is displayed on the Profile Settings page of the Settings dialog - see 2.3 (Profile Settings).

If a previous version of the identification file already exists, it will be overwritten. A confirmation dialog will be displayed asking you to verify that you want to do this.

For more information on the `ssh2.exe` command line version of the SSH Secure Shell client, see the Appendix A.1 (SSH2).

2.4.7 Certificates

Public Key Infrastructure (PKI) is a system where digital certificates are used to increase the reliability and scalability of authentication. Using certificate authentication requires that certificates are first created with certification authority (CA) software. For more information on certificates, see section 8.2 (Public-Key Infrastructure (PKI)).

Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.

The **Certificates** page (available only in commercial distributions) of the **Settings** dialog can be used to control certificates created by a certification authority (CA) software.

Certificate list

The available certificates are shown in the certificate list, located on the top of the **Certificates** page. The following fields are displayed on the certificate list:

Issued To

The **Issued To** field shows the entity to whom the certificate has been issued.

Issued By

The **Issued By** field shows the entity who has issued the certificate.

Expiration Date

The **Expiration Date** field shows when the certificate will expire.

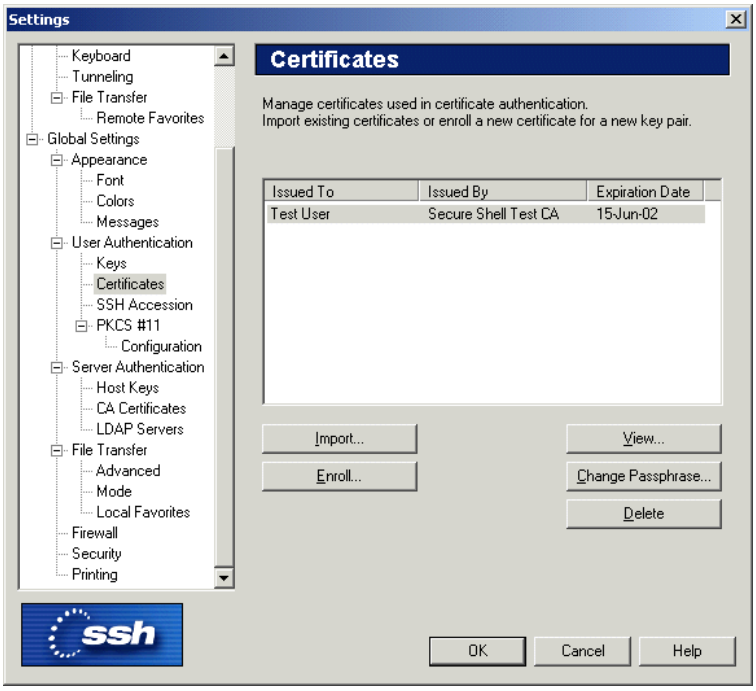

Figure 2.21: The Certificates page.

Buttons:

The following buttons can be used to control the certificates:

Import

Click the **Import** button to import a certificate created with certification authority (CA) software. A file selection dialog will open, allowing you to browse your directories for the saved certificate file.

Enroll

Click the **Enroll** button to start the **Certificate Enrollment** wizard, which is used to request a certification authority (CA) to issue a certificate. SSH Secure Shell supports the CMPv2 enrollment protocol.

For more information on the process, see section 2.4.8 (Certificate Enrollment Wizard).

Delete

Click the **Delete** button to remove a selected certificate.

View

Click the **View** button to display the contents of a selected certificate.

Change Passphrase

Click the **Change Passphrase** button to type a new passphrase associated with the selected certificate.

 © 2002 SSH Communications Security Corp.

2.4.8 Certificate Enrollment Wizard

The **Certificate Enrollment** wizard (available only in commercial distributions) is used to enroll certificates, i.e. to request a certification authority (CA) to issue a certificate. You can start the wizard by clicking on the **Enroll** button of the **Certificates** page of the **Settings** dialog.

Certificate Enrollment - Start

The first page of the **Certificate Enrollment** wizard displays information on the enrollment process. The enrollment process will create a key pair, consisting of a public and a private key. Please note that the process requires the use of Certificate Management Protocol version 2 (CMPv2).

Certificate Enrollment - Start
ssh
Certificate enrollment is an action wherein a CA certifies a public key.
This wizard will generate a private key and a public key which will be certified by a CA (Certification Authority). Only CMPv2 (Certificate Management Protocol) can be used
The private key and the enrolled certificate will be stored to the user settings folder. This key pair is used in public-key authentication.
< Back
Next >
Cancel
Help

Figure 2.22: The start of the enrollment process.

Click the **Next** button to continue the process.

Certificate Enrollment - Identity

On the **Identity** page, enter the parameters of the certificate to be issued. You can suggest a Common Name (e.g. *John Smith*), Organization Unit (like *Marketing*), Organization (*SSH Communications Security*), Country (*USA*) and Email Address (*john.smith@ssh.com*).

The certification authority can change these fields before issuing the certificate. The Certificate validity period and other parameters are determined by the configuration of the CA software.

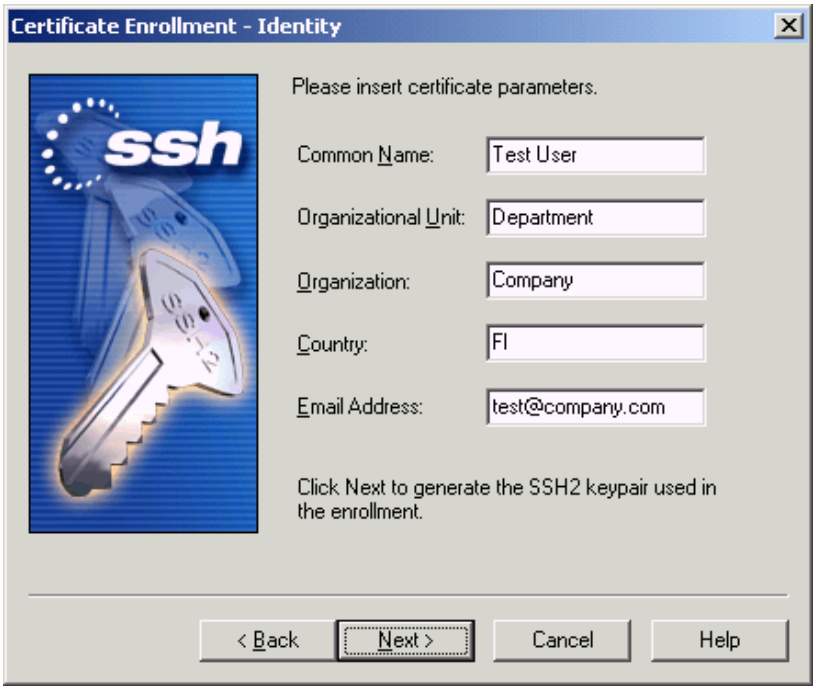

Figure 2.23: Type the parameters of the certificate.

Please note that certificate enrollment requiring manual acceptance in the CA software is not supported. You may be able to compensate for this by using PKCS #12 file importing.

Click the **Next** button to launch the Key Generation Wizard. For more information on the key generation process, see section 3.3.1 (Key Generation Wizard).

Certificate Enrollment - Firewall

On the **Firewall** page, you can define the firewall and proxy settings. If your local setup does not require these to be defined, the fields can be left empty.

Firewall

Type the firewall location in the text field.

HTTP proxy

Type the HTTP proxy location in the text field.

Click the **Next** button to continue.

 © 2002 SSH Communications Security Corp.

Certificate Enrollment - CA

On the **CA** page, fill in the following fields:

CMP Service URL

Type in the address of the server that provides the Certificate Management Protocol (CMP) service.

Discover

Click the **Discover** button to attempt automatic detection of available certification authority services and CA certificates. The found CA services will be listed in the text field and can be selected from the drop-down menu.

Please note that not all systems support the automatic detection functionality.

CA Certificate

This dropdown menu will be filled with the CA certificates that were found on the selected CMP service. Select a CA certificate from the list.

Alternatively, you can directly type in the file name of the certificate, or select the file by clicking on the button on the right hand side of the file name field. The **Select CA Certificate** dialog will open, allowing you to locate the certificate file.

View

Click the **View** button to display the contents of the current certificate.

Retrieve CA Certificates from CA URL

Select the desired CA URL from the drop-down list and click the **Retrieve CA Certificates from CA URL** button to retrieve the CA certificates from the selected CA address.

Reference Number

Type in the reference number.

Key

Type in the key information.

Click the **Next** button to continue.

Certificate Enrollment - Enrollment

On the **Enrollment** page the actual enrollment takes place. This may take some time (the exact duration depends on the amount of network traffic, among other factors).

When the process is finished, click the **Finish** button to continue.

Figure 2.24: The enrollment in progress.

2.4.9 SSH Accession

On the **SSH Accession** page of the **Settings** dialog you can operate the keys and certificates that are available on SSH Accession. SSH Accession is a separate software product by SSH Communications Security that offers an easy method for utilizing digital certificates and smart cards. For more information on SSH Accession, see `http://www.ssh.com/products/accession/`.

A 'lite' version of the SSH Accession software is included in the SSH Secure Shell distribution. For more information, see the *SSH Accession Lite User Manual*.

Go to SSH Accession

Click the **Go to SSH Accession** button to launch *SSH Accession*.

Upload Public Key

Select a public key from the list and click the **Upload Public Key** button to upload the key.

View Certificate

Select a certificate from the list and click the **View Certificate** button to display the contents of the certificate.

 © 2002 SSH Communications Security Corp.

Figure 2.25:

2.4.10 PKCS #11

The **PKCS #11** page (grayed out in non-commercial distributions) contains a list showing the configured PKCS #11 providers. Under each provider there is a list of the keys and certificates available. Please note that the list view does not get updated automatically, but only when you close and reopen it.

A new provider can be added to the list on the **Configuration** page of the **Settings** dialog. For more information, see section 2.4.11 (Configuration).

You can open the **PKCS #11** configuration window by double-clicking the card reader icon located on the right hand side of the SSH Secure Shell terminal window status bar, located on the bottom of the window.

Hardware tokens and PKCS #11 software keys can be used with or without PKI. The standard public-key authentication can be used with PKCS #11 providers.

The following buttons can be used to operate the PKCS # providers:

Enable Provider

Select a PKCS #11 provider from the list and click the **Enable Provider** button to allow the use of the selected provider.

Disable Provider

Select a PKCS #11 provider from the list and click the **Disable Provider** button to disallow the use of the selected provider.

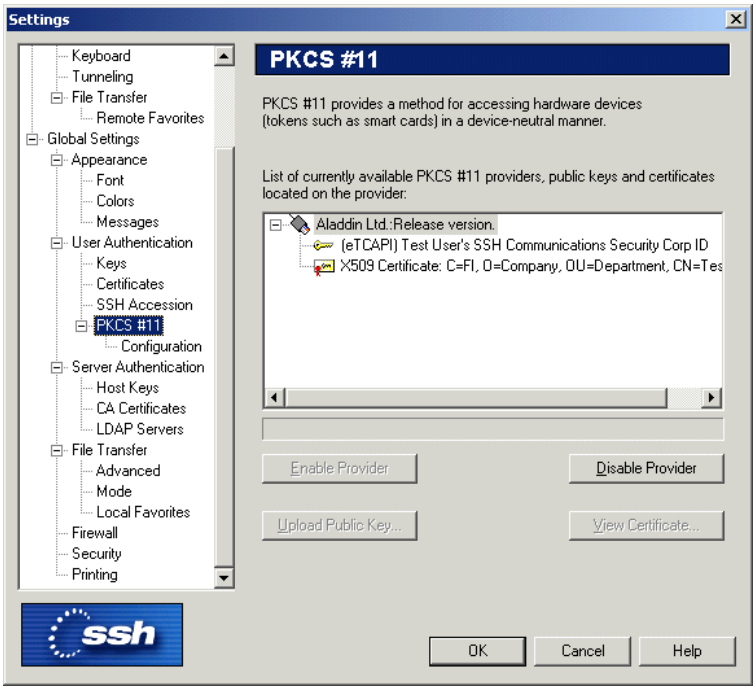

Figure 2.26: The PKCS #11 providers list.

Upload Public Key

Select a key from the list and click the **Upload Public Key** button to upload one of the public keys from the token to the server. This allows you to use a hardware token for your personal authentication. In order to do this, you have to be already connected to a server.

Please note that an RSA token requires RSA support to be compiled in the server software. See section 3.5 (Uploading Your Public Key) for information on how to upload a software public key to the server.

View Certificate

Click the **View Certificate** button to display the contents of the selected certificate.

2.4.11 Configuration

The **Configuration** page of the **Settings** dialog can be used to manually configure PKCS #11 providers.

The following fields are visible in the provider list, displayed on the top of the **Configuration** page:

Provider Type

The **Provider Type** field displays the type of the provider.

Initialization String

The **Initialization String** field displays the string of characters used for initialization.

 © 2002 SSH Communications Security Corp.

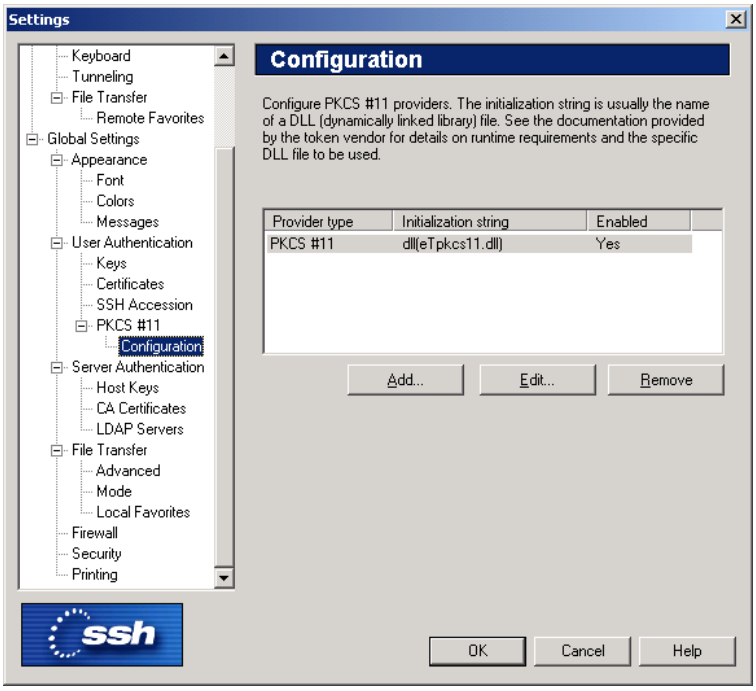

Figure 2.27: Configuring PKCS #11 providers.

Enabled

The **Enabled** field displays whether the use of the provider is currently allowed or not. To change the **Enabled** status, click the **Edit** button.

The following buttons can be used to control the provider settings:

Add

Click the **Add** button to add a new PKCS #11 provider. The **PKCS #11 Provider** dialog will open.

Edit

Click the **Edit** button to change the details of the PKCS #11 provider. The **PKCS #11 Provider** dialog will open.

Remove

Click the **Remove** button to delete the PKCS #11 provider definition.

For more information on the **PKCS #11 Provider** dialog, see section 2.4.12 (PKCS 11 Provider).

2.4.12 PKCS #11 Provider

The **PKCS #11 Provider** dialog allows you to view and modify the provider definition.

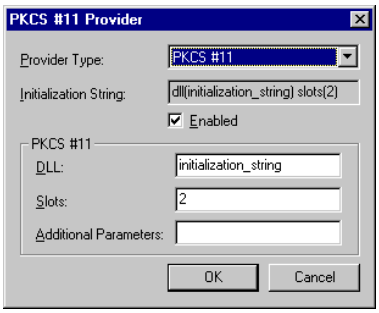

Figure 2.28: The details of the PKCS #11 provider displayed.

The following options are available:

Provider Type

Select the provider type from the dropdown menu.

Initialization String

This field displays the character string used for initialization.

Enabled

Leave the **Enabled** check box checked, except if you have trouble accessing the token from another application that is running simultaneously. The usability of a PKCS #11 for several simultaneous applications depends on the specific third party PKCS #11 driver.

PKCS #11

Fill in the following text fields to pass other parameters to the PKCS #11 provider:

DLL

Consult the token manufacturer documentation to determine the file name of the PKCS #11 DLL. Type this file name in the **DLL** field.

Slots

The Slots parameter is not required, but if you have problems accessing a specific key on a hardware token, you may need to modify this parameter accordingly. Consult the third party documentation for the exact requirements of the Slots parameter.

For example: to use PKCS #11 slots 0 through 10, use the value `0-10`, and to use slots 1 through 5 except 3, use the value `1-5,!3`.

Additional Parameters

Additional parameters can be specified, if specified in the third party documentation.

 © 2002 SSH Communications Security Corp.

When you save the settings (by using the **Save Settings** option on the **File** menu) and then restart SSH Secure Shell, you should see a small card reader icon on the status bar on the bottom of the terminal window. When a token is inserted, a smart card appears in the card reader in the icon. When a key is acquired from the token, a key symbol appears on top of the card reader icon.

If you do not see the card reader icon, check that the DLL name has been entered correctly. If you cannot get the keys from the token, make sure that the token has been personalized correctly. Please note that hardware tokens are usually shipped uninitialized, so you are required to personalize the token for yourself. To do this, you need to consult the third party documentation included with the token.

2.4.13 Server Authentication

There are two different methods that can be used to authenticate the server (remote host computer) you are connecting to: public-key authentication and certificate authentication.

Settings
Profile Settings
Connection
Cipher List
Authentication
Colors
Keyboard
Tunneling
File Transfer
Remote Favorites
Global Settings
Appearance
Font
Colors
Messages
User Authentication
Keys
Certificates
SSH Accession
PKCS #11
Configuration
Server Authentication
Host Keys
CA Certificates
LDAP Servers
File Transfer
Advanced
Server Authentication
The remote host can authenticate itself using either traditional public-key authentication or certificate authentication.
At the begining of the connection the server sends its public host key to the client for validation. If certificate authentication is used the public key is included in the certificate the server sends to the client.
In traditional public-key authentication the trust is based on the user verifying the fingerprint of the public host key when connecting for the first time to the remote host.
All subsequent connections to the remote host are authenticated using the public host key that was saved by the user to the local database.
When certificate authentication is used the client relies on a third party, a Trusted Certification Authority, to verify the remote host identity and issue a certificate for the host key pair.
The user won't have to verify the individual public host keys - only the Certification Authority certificate.
A Certificate Revocation List (CRL) is checked during certificate authentication to make sure the certificate has not been revoked. In traditional public-key authentication the user is responsible for managing the local public host key database.
ssh
OK
Cancel
Help

Figure 2.29: The Server Authentication page of the Settings dialog.

When *public-key authentication* is used to authenticate the server, the first connection is very important. The client will ask the user to save the host key to the local database. The fingerprint of the public key should be verified before you save it to the local database and proceed with the connection. If you do not verify the authenticity of the fingerprint, you risk the possibility of a man-in-the-middle attack. For future connections, the local copy of the server's public key will be used in server authentication.

Certificate authentication is more secure than the traditional public-key authentication, as the system verifies that the server certificate has been issued by a trusted Certificate Authority (CA) and that the certificate has not been revoked. When certificate authentication is used, the man-in-the-middle attack is no longer a threat

during key exchange, as the system verifies that the server certificate has been issued by a trusted certification authority (CA).

If the server certificate itself does not contain a valid authority information access or a CRL distribution point extension, an LDAP server has to be configured on the client-side to obtain a certificate revocation list (CRL).

Note: Certificate authentication is supported only in the commercial versions of SSH Secure Shell.

2.4.14 Host Keys

Public host keys used in server authentication (remote host authentication) process can be managed using the **Host Keys** page of the **Settings** dialog. The keys are listed in the host key file list.

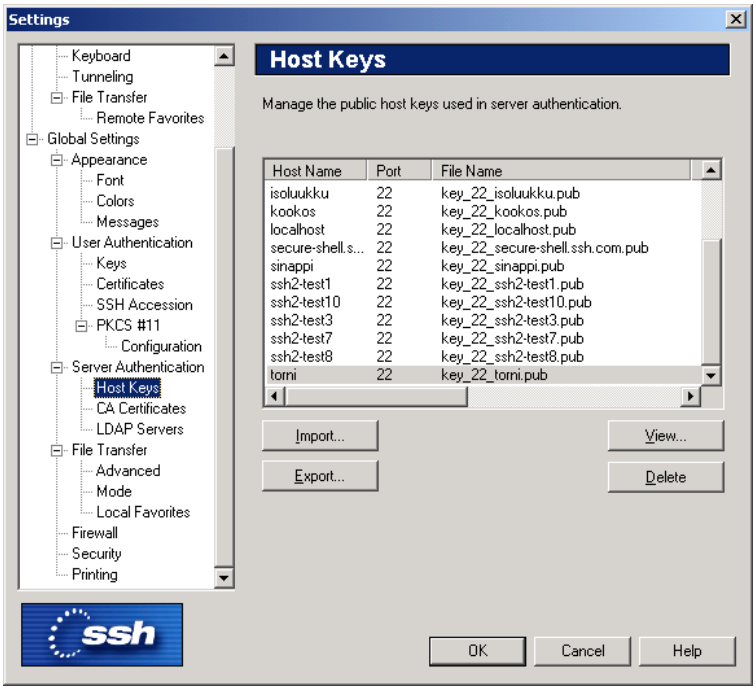

Figure 2.30: The Host Keys page of the Settings dialog.

Public host key file list

The host keys in your possession are displayed in the public host key file list (located above the buttons on the **Public Keys** page).

Host Name

The **Host Name** column displays the host names of your host keys.

Port

The **Port** column displays the ports used by the connections associated with each host key.

File Name

The **File Name** column displays the file name of each host key file.

Fingerprint

The **Fingerprint** column displays the fingerprint of each host key file. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable sets of five lowercase letters separated by dashes.

Buttons:

View

Select a host key file from the host key file list and click the **View** button to display a host key. Alternatively you can just double-click on the key file name.

Export Key

Select a host key and click the **Export Key** button to export a host key. The **Select Folder** dialog will open, allowing you to specify the target location.

Import Key

Click the **Import Key** button to import a host key. The **Import Hostkeys - Select Files** dialog will open, allowing you to locate the host key to be imported.

Delete

Select a host key file from the host key file list and click the **Delete** button to remove the key.

2.4.15 CA Certificates

On the **CA Certificates** page of the **Settings** dialog you can manage the certificates of your trusted certification authorities (CA). For more information on certificates, see section 8.2 (Public-Key Infrastructure (PKI)).

Please note that certificate support is only available in commercial distributions of the SSH Secure Shell for Workstations client.

CA certificate list

The available CA certificates are shown in the CA certificate list, located on the top of the **CA Certificates** page.

The following fields are displayed on the CA certificate list:

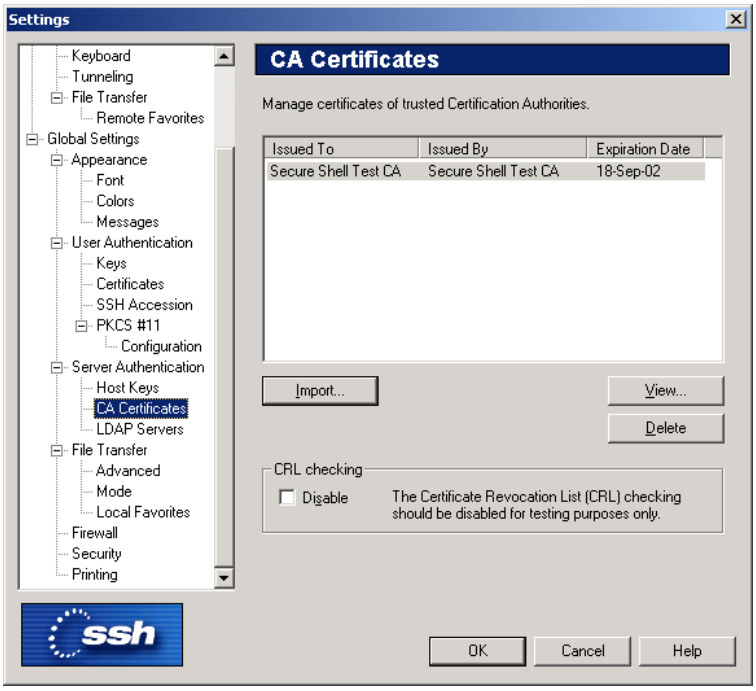

Figure 2.31: A brief overview of PKI.

Issued To

The **Issued To** field shows the certification authority to whom the certificate has been issued.

Issued By

The **Issued By** field shows the entity who has issued the CA certificate.

Expiration Date

The **Expiration Date** field shows when the CA certificate will expire.

Buttons:

The following buttons can be used to control the CA certificates:

Import

Click the **Import** button to import a CA certificate from an external file. The **Import Certificate - Select File** dialog will opened, allowing you to locate the certificate file.

View

Click the **View** button to display the contents of a selected CA certificate.

Delete

Click the **Delete** button to remove a selected CA certificate.

CRL Checking

Select the **Disable** check box to prevent the use of a certificate revocation list (CRL). A CRL is used to check if any of the used CA certificates have been revoked.

Note: Disabling CRL checking is a security risk and should be done for testing purposes only.

2.4.16 LDAP Servers

In order to make use of a certificate, it must be distributed to directories where it is made available to other users. SSH Secure Shell supports certificate and certificate revocation lists (CRL) distribution using the Lightweight Directory Access Protocol (LDAP), a de facto standard. This enables interoperability with third party directory servers using the LDAP standard.

For more information on LDAP, see section 8.2.4 (Directory Services).

(Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.)

The **LDAP Servers** list displays the available LDAP servers.

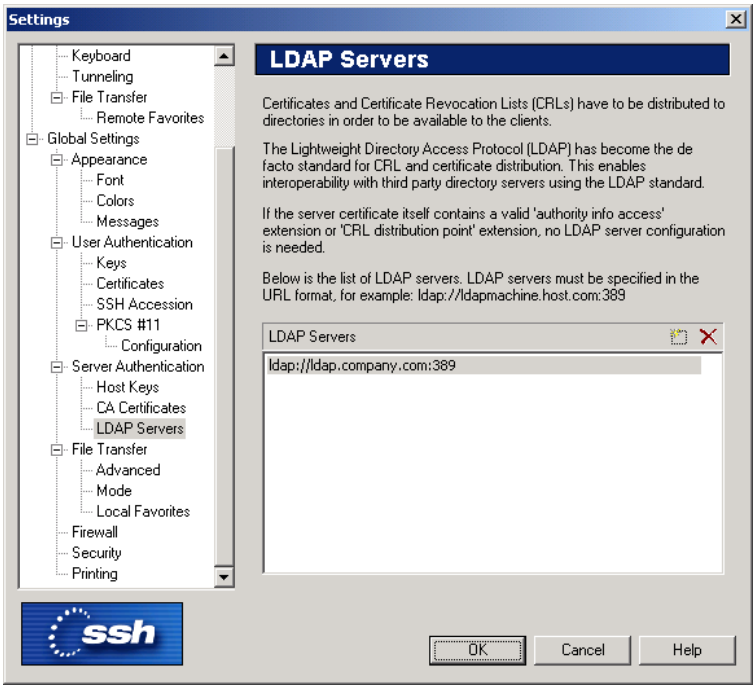

Figure 2.32: Adding a new LDAP server entry.

To edit an LDAP server entry, doubleclick the appropriate line in the list. To add or delete LDAP server entries, use the buttons located above the LDAP server list:

New

Click the **New** button (the leftmost button on the top right hand side of the LDAP server list) to add a new LDAP server to the list. Type in the address of the server using URL format (for example `ldap://ldap.host.com:389`). The keyboard shortcut for the New button is the `Ins` key.

Delete

Select an unwanted LDAP server entry from the list and then click the **Delete** button (the rightmost button on the top right hand side of the LDAP server list) to remove the server definition. The keyboard shortcut for the Delete button is the `Delete` key.

2.4.17 File Transfer

The default file transfer settings can be configured using the **File Transfer** page of the **Settings** dialog. The new settings will affect subsequently started File Transfer windows.

Figure 2.33: The global File Transfer page of the Settings dialog.

Show Root Directory

Select the **Show Root Directory** check box to show the root directory in the **File Transfer** window by default.

Show Hidden Files

Select the **Show Hidden Files** check box to show hidden files in the **File Transfer** window by default.

Check and Confirm Overwrite

Select the **Check and Confirm Overwrite** check box if you want the File Transfer utility to ask for confirmation when you try to transfer a file that already exists in the target system.

Display Items by Using

With the **Display Items by Using** setting you can select the default view for the File Transfer window by choosing one of the four possible views.

Large Icons

Select the **Large Icons** option to display the File Transfer file view as a Large Icons view. Each file and folder has a large icon associated with it, making for a clear and uncluttered display.

Small Icons

Select the **Small Icons** option to display the File Transfer file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

List

Select the **List** option to display the File Transfer file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

Details

Select the **Details** option to display the File Transfer folder view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, their last modification date and attributes visible.

By clicking on the **Name**, **Size**, **Type**, **Modified** and **Attributes** sort bars located on top of the File view, you can sort the files and folders based on their file name, file size, file type and the time they were last modified. Clicking the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file type associations are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the host computer.

Missing File Association

The SSH Secure Shell for Workstations Windows client uses file type associations in the same way as Windows Explorer does. When you double-click a file in the File Transfer window, it will be opened using the application with which its file type has been associated.

All file types are not associated with any application. With this field you can define what application will be used to open a file that has no file type association. The default application is *Notepad*, which is a reasonable choice for files containing text.

To change the default association for unknown file types, click the button next to the text field. A Select Application dialog will be displayed, allowing you to select the desired application.

Formatting string for file time

In the formatting string field you can type a string that presents how the time and date stamps of the files are displayed in the File Transfer window. The default value is `%c`, which means that the date and time will be presented in the format defined in the Windows country settings (locale).

To change the format of the time and date stamps, replace the default value with a string consisting of some of the following character combinations.

%a

Abbreviated weekday name

%A

Full weekday name

%b

Abbreviated month name

%B

Full month name

%c

Date and time representation appropriate for locale

%d

Day of month as decimal number (01 - 31)

%H

Hour in 24-hour format (00 - 23)

%I

Hour in 12-hour format (01 - 12)

%j

Day of year as decimal number (001 - 366)

%m

Month as decimal number (01 - 12)

%M

Minute as decimal number (00 - 59)

 © 2002 SSH Communications Security Corp.

%p

Current locale's A.M. / P.M. indicator for 12-hour clock

%S

Second as decimal number (00 - 59)

%U

Week of year as decimal number, with Sunday as first day of week (00 - 53)

%w

Weekday as decimal number (0 - 6; Sunday is 0)

%W

Week of year as decimal number, with Monday as first day of week (00 - 53)

%x

Date representation for current locale

%X

Time representation for current locale

%y

Year without century, as decimal number (00 - 99)

%Y

Year with century, as decimal number

%z, %Z

Time-zone name or abbreviation; no characters if time zone is unknown

%%

Percent sign

View Layout

You can select how the **File Transfer** window positions the local and remote view panes. The following options are available:

Remote view on top, local view on bottom

Remote view on right, local view on left

Remote view on left, local view on right

Wide folder view on file bar

Select this checkbox to show fewer buttons on the file bar, leaving more room for the favorite folders lists.

2.4.18 Advanced

On the **Advanced** page of the **Settings** dialog you can configure additional file transfer options. The new settings will affect subsequently started File Transfer windows.

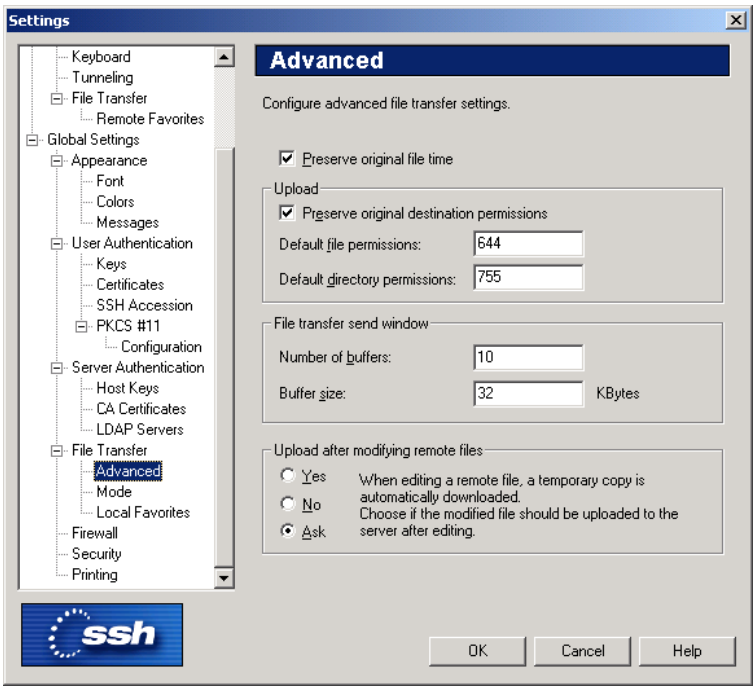

Figure 2.34: The advanced file transfer options.

Preserve Original File Time

Select the **Preserve Original File Time** check box if you want that the transferred files retain their original time and date stamp values. If this option is not selected, the transferred files will be stamped with the time of the transfer.

Upload

The following settings affect the upload process:

Preserve Original Destination Permissions

Select this check box to preserve the file permissions of the original file located on the remote host computer. The transferred file will use the same file permissions as the original file.

Default File Permissions

Type the octal UNIX file permission mask (as with the UNIX `chmod` command) that is to be used as the default value for files. For more information on file permissions, see section 5.1.5 (Contents of the File Transfer Window).

 © 2002 SSH Communications Security Corp.

Default Directory Permissions

Type the octal UNIX directory permission mask (as with the UNIX `chmod` command) that is to be used as the default value for directories.

File Transfer Send Window

The following settings affect the file transfer process:

Number of Buffers

Type the number of buffers used in file transfer. The default value is 10.

Buffer size

Type the default buffer size (measured in kilobytes). The default value is 32 kilobytes.

Upload Locally Modified Remote Files

This selection affects how SSH Secure Shell will react if you edit locally a file stored in the remote host computer.

Yes

If you select the **Yes** option, the locally modified file will be uploaded to the remote host computer.

No

If you select the **No** option, the locally modified file will not be uploaded to the remote host computer.

Ask

If you select the **Ask** option, SSH Secure Shell will ask you to decide if you want to upload a locally modified file.

2.4.19 Mode

The **Mode** page of the **Settings** dialog affects which files will be transferred using ASCII mode.

File Transfer Mode

Select the default file transfer mode from the following options:

ASCII

By default all files will be transferred in ASCII mode.

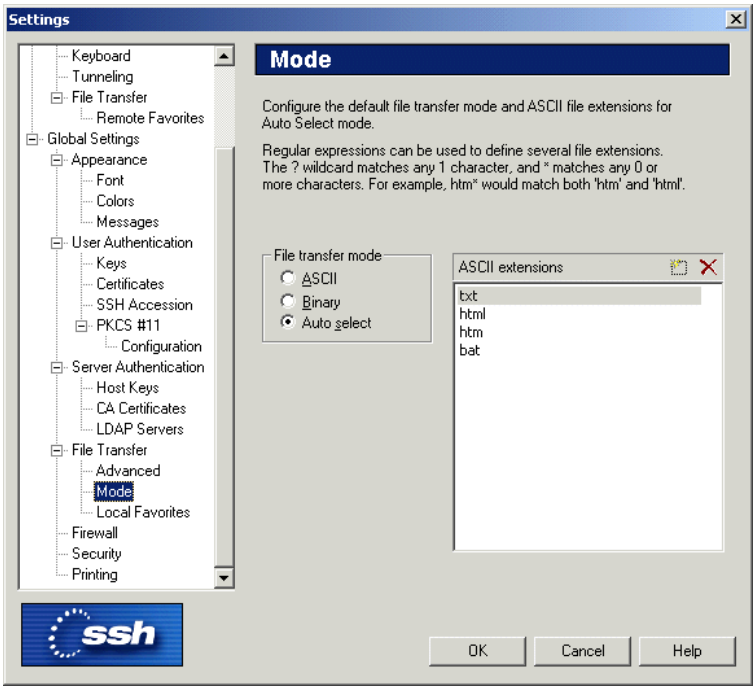

Figure 2.35: Selecting the file transfer mode.

Binary

By default all files will be transferred in binary mode.

Auto Select

The files using a file extension specified on the ASCII Extensions list will be transferred in ASCII mode. All other files will be transferred in binary mode.

ASCII Extensions

Files using a file extension specified in the ASCII Extensions list will be transferred using ASCII mode.

New

Click the **New** button (the leftmost button on the top right hand side of the ASCII Extensions list) to add a new file extension to the list. The keyboard shortcut for the New button is the `Ins` key.

Note that you can use wild cards to specify the file extensions. The `?` character matches any 1 character, and the `*` character matches any 0 or more characters. (For example: `htm*` would match both `htm` and `html`.)

Delete

Select an unwanted file extension entry from the list and then click the Delete button (the rightmost button on the top right hand side of the ASCII Extensions list) to remove the extension. The keyboard shortcut for the **Delete** button is the `Delete` key.

 © 2002 SSH Communications Security Corp.

2.4.20 Local Favorites

On the **Local Favorites** page of the **Settings** dialog you can create a list of commonly used directories on your local computer. These favorites can then be easily selected from a drop-down menu in the File Transfer window.

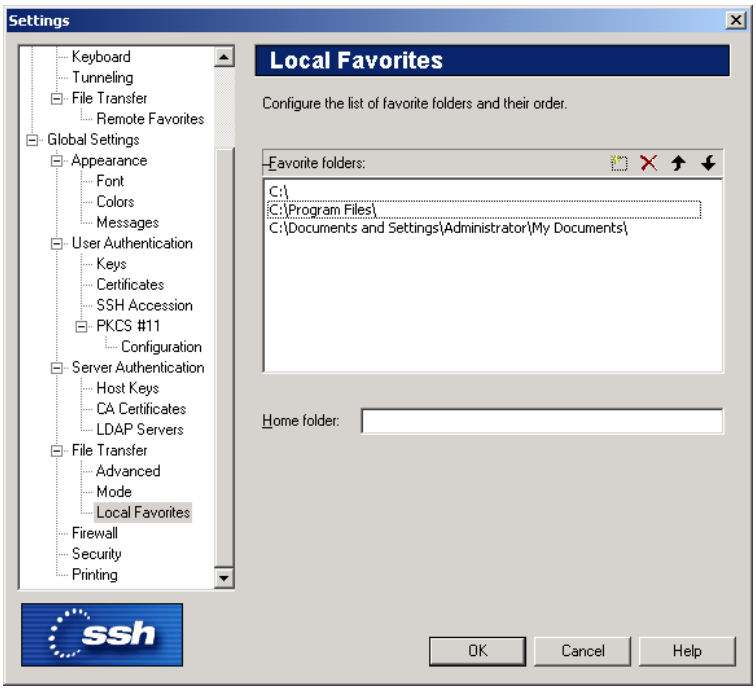

Figure 2.36: Creating a list of most commonly used directories.

Favorite Folders

This list contains the favorite folders you have defined for your local computer. Initially the list contains your locally available drives. You can add, remove and sort the favorites by using the icons displayed above the list:

New

Click the **New** button to add a new favorite, and then type the path to the desired folder.

Delete

Select an already defined favorite from the list and then click the **Delete** button to remove it from the list.

Up

Select an already defined favorite from the list and then click the **Up** button to move it higher in the list.

Down

Select an already defined favorite from the list and then click the **Down** button to move it lower in the list.

Home Folder

In the **Home Folder** field you can type the directory that is initially displayed in the local view pane of the File Transfer window.

2.4.21 Firewall

The firewall settings can be configured using the Firewall page of the Settings dialog. The firewall should run SOCKS version 4 or 5 software.

Note: SOCKS5 authentication or encryption functionality is not supported.

Connecting through a firewall requires that the **Connect through Firewall** option on the **Connection** page has been selected. For more information, see section 2.3.1 (Connection).

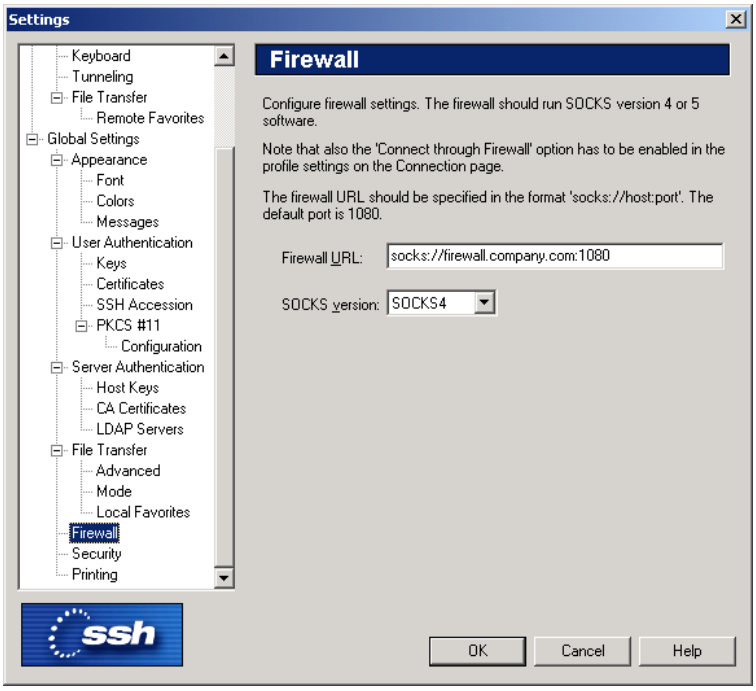

Figure 2.37: The Firewall page of the Settings dialog.

Firewall URL

Type the firewall address in URL format (for example `socks://host.computer:1080`). The default port is 1080.

 © 2002 SSH Communications Security Corp.

SOCKS Version

Select the SOCKS version used by the firewall. Available options are SOCKS4 and SOCKS5.

2.4.22 Security

The security settings can be configured using the **Security** page of the **Settings** dialog.

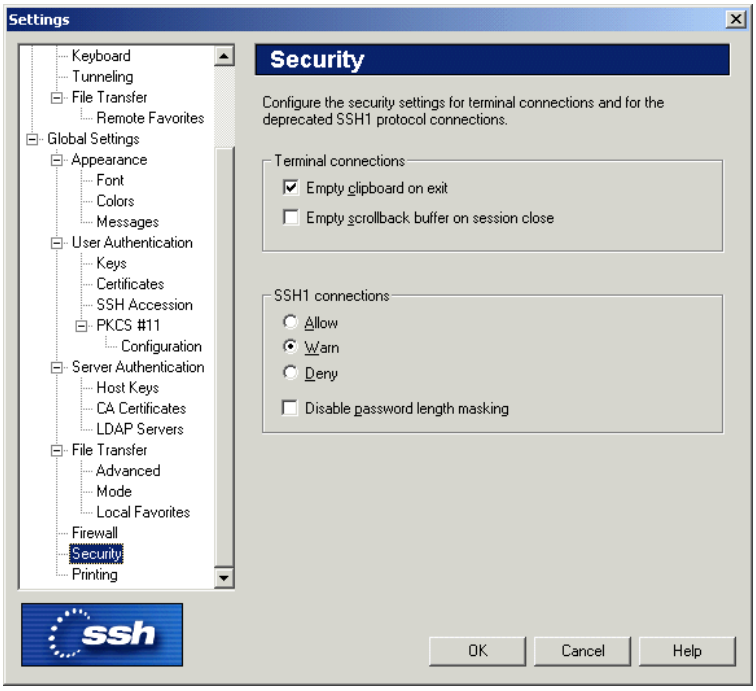

Figure 2.38: The Security page of the Settings dialog.

Empty Clipboard on Exit

Select the **Empty Clipboard on Exit** check box to remove from the clipboard anything that was recently copied using the cut and paste Edit operations.

Empty Scrollback Buffer on Session Close

Select the **Empty Scrollback Buffer on Session Close** check box to empty any remains of the terminal output from the scrollback buffer.

SSH1 Connections

From SSH Secure Shell for Workstations Windows client version 2.2.1 onwards, you can connect also to Secure Shell version 1 (SSH1) servers. With the SSH1 Connections selection you can decide if you want to allow SSH1 connections, deny them, or issue a warning when connecting to a remote host computer that is using version 1 of the Secure Shell protocol.

Secure Shell version 2 (SSH2) is a more advanced and secure protocol than the legacy version SSH1. For more information on the status of the SSH1 protocol, see the SSH web site `http://www.ssh.com/products/ssh/deprecation.cfm`.

Note that when using an SSH1 connection, multiple terminal windows and the file transfer operations are not available.

Allow

Select this option to allow also SSH1 connections.

Warn

Select this option to issue a notice when an SSH1 connection is made.

Deny

Select this option to disallow SSH1 connections.

Disable password length masking in SSH1 connections

Select this check box to not use password length masking when logging in using the SSH1 protocol.

2.4.23 Printing

The print settings can be configured using the **Printing** page of the **Settings** dialog.

Printer Font

Select the **Font Name** and **Font Size** to be used in the printed output. Any non-proportional font installed on your system can be selected.

Margins (mm)

Select the width of the blank border around the page on printed output. The margins for the top, bottom, left and right of the page can all be specified individually. The default value for all margins is 10 millimeters (or 1 centimeter).

Header & Footer

Select what additional information appears on the printed pages.

Title appears at the top left of the page and displays the title of the terminal window (for example: `remotehost - SSH Secure Shell`).

Date appears at the top right of the page and displays the date and time when the page was printed (for example: `10 May 2002, 23:27`). The date and time format is the same as used in Windows.

Page Number appears at the bottom right of the page (for example: `Page 1 of 2`).

 © 2002 SSH Communications Security Corp.

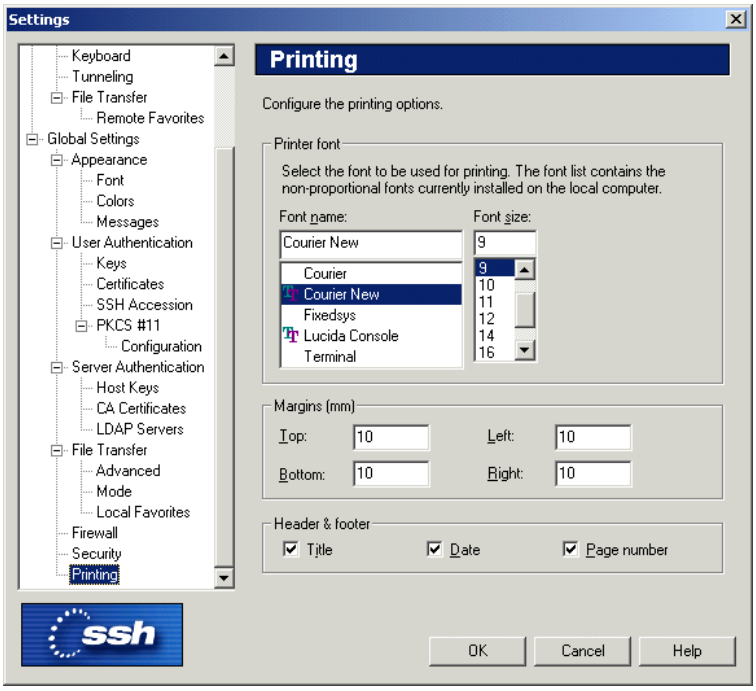

Figure 2.39: The Printing page of the Settings dialog.

2.5 Customize

Select the **Customize** option from the **View** menu to modify the menu options, toolbars layout, keyboard mapping, menu settings and general preferences. Note that you can have only one terminal window open when using the Customize option.

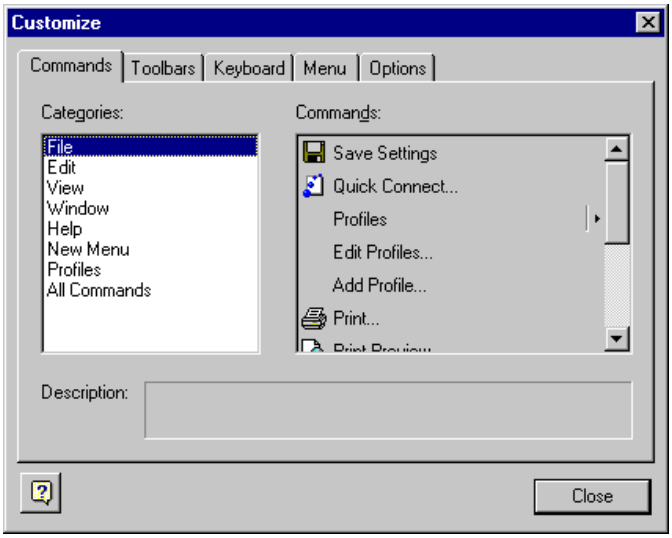

Figure 2.40: Use the Customize dialog to modify the user interface settings.

Click on the tabs on the top of the dialog to switch between different pages:

Commands tab

Select the **Commands** tab to move individual menu options. Select the menu category from the list on the left, and then use the mouse to drag menu options into the menus or toolbars displayed in the SSH Secure Shell window.

Toolbars tab

Select the **Toolbars** tab to define which toolbars are displayed on the SSH Secure Shell window.

If you have made any changes, you can select the toolbars you want reset and then click the **Reset** button to return the default toolbar configuration. Click the **Reset All** button to reset all the toolbars and menus.

Reset

Select a toolbar that you want to restore to its initial settings and then click the **Reset** button to discard the changes you have made.

Reset All

Click the **Reset All** button to discard the changes you have made to all of the toolbars.

Show Text Labels

Select either the **Profiles** or the **Toolbar** option and then select the **Show text labels** check box to display text labels on these toolbars. Text labels clarify the toolbar icons, but also take up space.

Keyboard tab

Select the **Keyboard** tab to define accelerator keys (keyboard shortcuts) for the menu commands.

Use the **Category** menu to select the category of the accelerator key you want to modify. The categories are based on the menu hierarchy.

Use the **Commands** menu to select a specific command from the selected category.

The **Description** box displays a brief description of the currently selected command.

Use the **Set Accelerator for** menu to select the profile that you want to associate with the current keyboard configuration.

The **Current Keys** field shows the currently assigned accelerator keys.

Click on the **Press New Shortcut Key** field to activate it. Then press the combination of keys on the keyboard that you want to associate with the currently selected command.

Assign

Click the **Assign** button the add the definition from the Press New Shortcut Key field to the Current Keys field.

Remove

Select a key assignment from Current Keys field and click the **Remove** button to delete the selected assignment.

Reset All

Click the **Reset All** button to lose all your changes and reset the keyboard assignments. A confirmation dialog will be displayed, asking if you really want to do this.

 © 2002 SSH Communications Security Corp.

Menu tab

Select the **Menu** tab to define the menu settings.

Application Frame Menus

Select the menu setup you want to change from the **Show Menus For** dropdown menu. By default, only the *Default Menu* is available for editing.

Click the **Reset** button to reset the menus to their original configuration.

Use the **Menu animations** dropdown menu to select the type of menu animations. The available options are None, Unfold, Slide and Fade.

Select the **Menu shadows** check box to display shadows under open menus.

Context Menus

Use the **Select context Menu** dropdown menu to display any of the shortcut (or popup) menus:

- File Local Menu 1 (displayed in the local view of the File Transfer window when you do not have a file selected)
- File Local Menu 2 (displayed in the local view of the File Transfer window when you have a file selected)
- File Remote Menu 1 (displayed in the remote view of the File Transfer window when you do not have a file selected)
- File Remote Menu 2 (displayed in the remove view of the File Transfer window when you have a file selected)
- Terminal Popup menu (displayed when you right-click in the terminal window).

Then you can click the Commands tab and drag menu options into the shortcut menus (and remove items from the shortcut menus by dragging them off the menu).

Reset

Click the **Reset** button to reset the menus to their original configuration.

Options tab

Select the **Options** tab to change general user interface options.

Select the **Show Screen Tips on toolbars** check box to display a short help text, when you place the mouse pointer over a toolbar button.

Select the **Show shortcut keys in Screen Tips** check box to see the possible keyboard shortcut displayed in addition to the short help text.

Select the **Large Icons** check box to display big toolbar icons.

Select the **Look 2000** check box to enable Windows 2000 style features in the user interface. This option affects mainly the style of the toolbar handles.

Help

Click the **Help** button to display the online help.

Close

Click the **Close** button to stop the customization process.

Chapter 3

Connecting

SSH Secure Shell makes it easy to establish connections to new remote host computers, and to manage the settings required for each different host.

The Quick Connect option allows you to create new connections fast, minimizing the hassle associated with configuring each connection. It is easy to define a profile for new hosts, and save just the right settings for each.

3.1 Quick Connect

Select the **Quick Connect** option (from the toolbar or from the File menu) to establish a completely new SSH connection that can be operated independently of any other clients and connections. You can connect to an entirely new remote host computer and still keep the old connection to a different host open.

The **Connect to Remote Host** dialog will open, automatically filled in with the values defined in the default configuration file (`default.ssh2`). Therefore it makes sense to use the Settings dialog (see section 2.1 (Saving Settings)) to set the most commonly used options and save them in the `default.ssh2` configuration file.

When you need to establish a new connection, just click the Quick Connect button to connect to a new host with the default settings. When connected, you can then customize the settings to match your exact requirements for this particular host and save the settings as this host's profile (see section 3.2 (Profiles)).

But there is an even faster alternative. When you login using the default settings, the Add Profile dialog is briefly and non-intrusively shown. Click on the dialog and write in the name for the new profile. When you press the Enter key, the profile is automatically saved. It is accessible from the Profiles menu, and can later be fully customized.

 © 2002 SSH Communications Security Corp.

3.2 Profiles

If you habitually connect to more than just one remote host computer, you probably want to have different settings defined for each host. Profiles make it easy to manage different host configurations.

You can have an unlimited amount of different profiles customized for different connections.

Note that the SSH Secure Shell for Workstations Windows client considers the profiles as the user's personal data and saves the profile definition files in the personal folder of the user. This means that every user of the local computer can have his or her own profiles, without affecting other users of the same computer.

Select the Profiles option (from the toolbar or the File menu) to either add a new profile definition or edit an already defined profile.

3.2.1 Add Profile

Adding a new profile is extremely easy. When you have connected to a new host computer, select the Add Profile option. The Add Profile dialog will open.

Figure 3.1: Just type in a name for the new profile and you are ready!

Type a name for the profile (the name of the host computer is a good choice) and press Enter. You are ready!

When you later want to connect to the same host, just select its profile under the Profiles option. You will be immediately connected, with all the settings in their proper places - even including the number and positions of SSH Secure Shell windows.

By using profiles, you can have just the right connection settings for each host, with no hassle or defining complicated configuration settings. It's that simple.

3.2.2 Edit Profiles

Click the Edit Profiles option to modify profiles that you have saved earlier. The Edit Profiles dialog will open, allowing you to edit all the host specific settings associated with this particular connection.

Click on the tabs on the top of the page to switch between pages. For a closer look on the settings displayed under each tab, see sections 2.3.1 (Connection), 2.3.2 (Cipher List), 2.3.3 (Authentication), 2.3.5 (Keyboard), 2.3.4 (Colors), 2.3.7 (Tunneling), 2.3.8 (File Transfer) and 2.3.9 (Remote Favorites).

You can make changes to several profiles at the same time by changing the profile with the profile tree displayed on the left hand side of the Edit Profiles dialog.

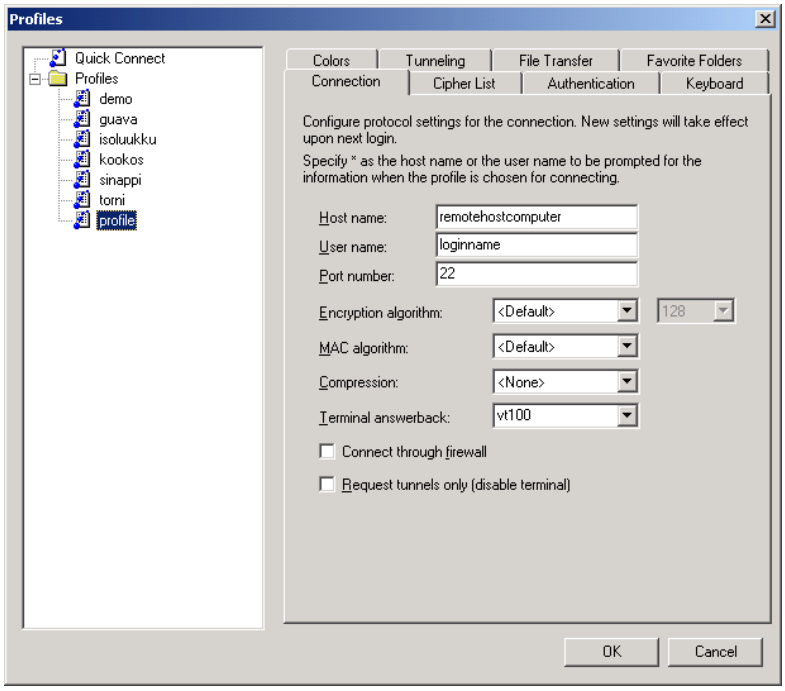

Figure 3.2: Use the Profiles dialog to customize settings for each host computer.

When you are finished with the settings, you can click the OK button to save the new profile definition, or the Cancel button to change your mind and abort your changes.

Note: Before the profile editing operation, the `.ssh2` settings are copied into backup files with the file extension `.bak`. If you remove these backup files, you will not be able to revert back to the old settings.

Profiles Shortcut Menu

Click the profile tree with the right mouse button, and a shortcut menu will open.

If you right-click on a profile, you can select from the following options:

Connect

Select the Connect option to immediately connect to the remote host computer associated with the profile.

Copy

Select the Copy option to copy the profile definition into the clipboard. Now you can click an empty location in the profile tree and paste a copy of the profile there.

Cut

Select the Cut option to remove the profile from its present location in the profile tree. Now you can click an empty location in the profile tree and paste the profile there.

 © 2002 SSH Communications Security Corp.

Delete

Select the **Delete** option to remove the profile. A **Confirm Delete** dialog will open, asking if you are sure that you want to erase the selected profile.

Rename

Select the **Rename** option to type in a new name for the profile. It is a good idea to give each profile a descriptive name, so that the profiles are easy to recognize later on.

Create Shortcut

Select the **Create Shortcut** option to create a shortcut to the currently defined profile on the Windows desktop. The shortcut will be have the name of the current profile (typically the remote host computer that you are connected to). When you later click on the shortcut, SSH Secure Shell will be launched with the settings that have been saved for the profile.

If you right-click on an empty spot on the profile tree, you can select from two options:

Paste

Select the Paste option to paste a profile that you have copied.

New Folder

Select the New Folder option to create a new folder in the profile tree.

Organizing Profiles

If you have defined a long list of profiles, it may be a good idea to organize them into folders. Click the profile list with the right mouse button, and select the New Folder option to create a new folder in the profile tree structure. Type a name for the new folder.

Now you can use the mouse to drag and drop the profiles and arrange them into folders so that you can quickly find the profiles you need.

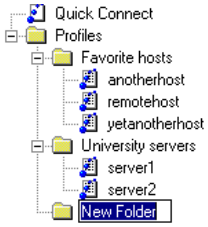

Figure 3.3: Creating a new folder for better organization.

3.3 Key Generation

If you are going to connect to a remote host computer using public-key authentication, you will have to generate your key pair before connecting.

Public-key authentication is based on the use of digital signatures. Each user creates a pair of 'key' files. One of these key files is the user's public key, and the other is the user's private key. The server knows the user's public key, and only the user has the private key.

When the user tries to authenticate herself, the server checks for matching public keys and sends a challenge to the user end. The user is authenticated by signing the challenge using her private key.

Remember that your private key file is used to authenticate you. Never expose your private keys. If anyone else can access your private key file, they can attempt to login to the remote host computer as you, and claim to be you. Therefore it is extremely important that you keep your private key file in a secure place and make sure that no one else has access to it.

Do not use public-key authentication on a computer that is shared with other users. Generate keys only on your personal computer that no one else can access!

In order to use public-key authentication, you must first generate your own key pair. You can generate your own key files with the help of a built-in key generation wizard.

3.3.1 Key Generation Wizard

To generate a new key pair, open the **Settings** dialog and select the **Keys** page (in the **User Authentication** branch). Then click the **Generate New Keypair** button to run the key generation wizard.

The wizard will generate two key files, your private key and your public key. The private key file has no file extension, and the public key has the same base file name as the private key, but with `.pub` as the file extension. The key files will be stored in your local computer, in the user profile directory.

3.3.2 Key Generation - Start

The Key Generation - Start page contains important information about safety measures. Read the text and click the Next button.

3.3.3 Key Generation - Key Properties

On the **Key Properties** page, select the type of the key to be generated. You can select to generate either an RSA or a DSA key, as well as the key length.

Key Type

 © 2002 SSH Communications Security Corp.

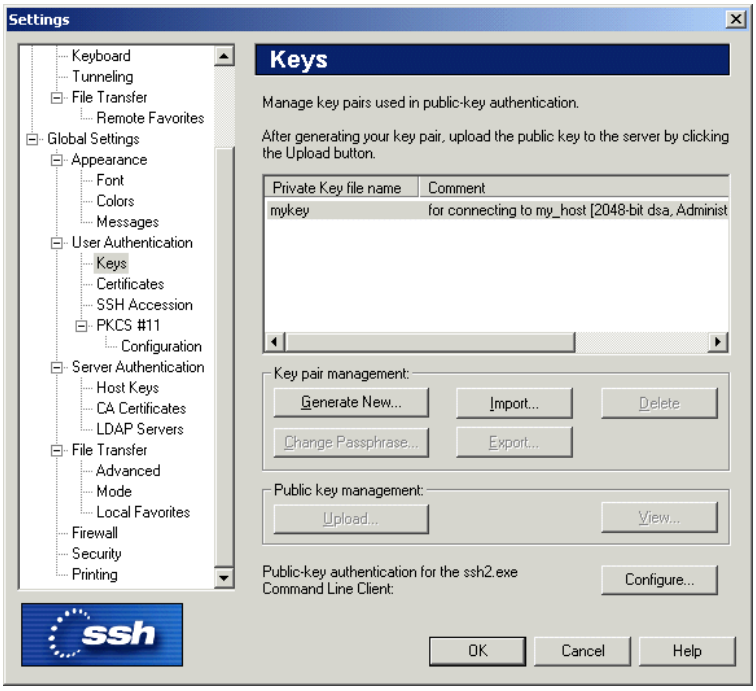

Figure 3.4: The Keys page with a key pair already generated.

Key Generation - Start
ssh
This wizard will generate a new pair of SSH2 keys to be used for public key authentication.
Two key files will be generated, a private key file, which has no file name extension, and a public key file which has the same name as the private key file but with the file name extension ".pub".
The files will be stored in user settings folder on the local disk.
Please note that it is not safe to use public key authentication on a public computer that can be used by several users. Generate keys only on personal computer no one else has access to.
Keep your private keys protected and never expose them.
< Back
Next >
Cancel
Help

Figure 3.5: The Start page of the key generation wizard.

Select the type of the key to be generated. Available options are DSA or RSA.

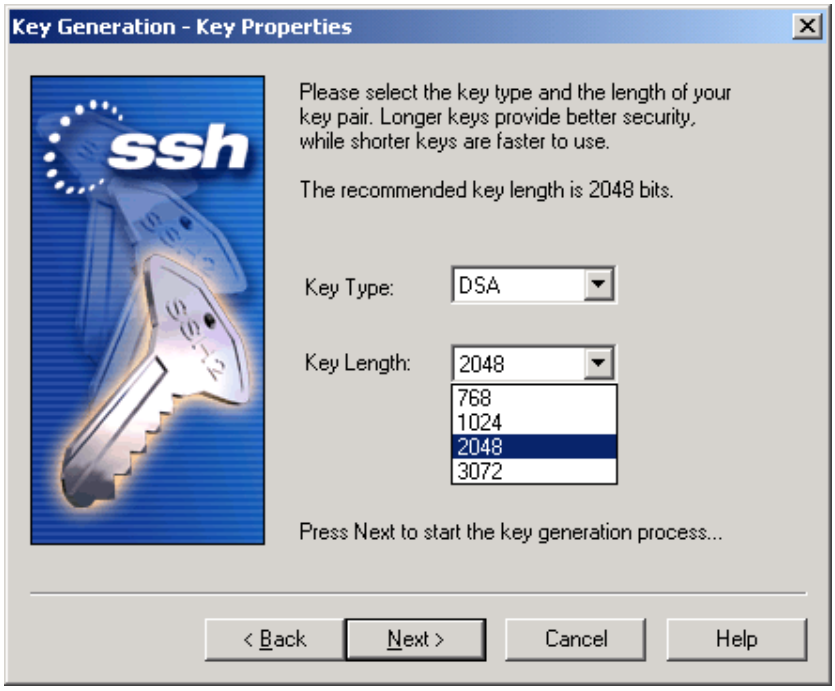
Key Generation - Key Properties
Please select the key type and the length of your key pair. Longer keys provide better security, while shorter keys are faster to use.
The recommended key length is 2048 bits.
Key Type:
DSA
Key Length:
2048
768
1024
2048
3072
Press Next to start the key generation process...
< Back
Next >
Cancel
Help

Figure 3.6: Selectin the key type

Key Length

Select the length (complexity) of the key to be generated. Available options are 768, 1024, 2048 or 3072 bits. Larger keys are more secure, but also slower to use. The recommended key length for most occasions is 2048 bits.

3.3.4 Key Generation - Generation

On the Key Generation - Generation page the computer will generate your key files. This can take several minutes, depending on the chosen key length and the processor speed of the computer.

During the key generation phase an animation of random bits is displayed. When the process is ready, the Next button is ungrayed and you can proceed to the next phase by clicking it.

3.3.5 Key Generation - Enter Passphrase

On the Key Generation - Enter Passphrase page you can provide information describing the generated key pair, and protect the files with a passphrase.

File Name

Type a name for the key file in the File Name field.

 © 2002 SSH Communications Security Corp.

Key Generation - Generation
Key generation is now in progress. The generation may take several minutes depending on the processor speed of the computer and the chosen key length. Please wait until the generation is complete.
< Back
Next >
Cancel
Help

Figure 3.7: Key generation in process.

Key Generation - Enter Passphrase
Please provide a file name for the private key, a comment (to help recognise the key) and a passphrase.
The private key will be encrypted. A passphrase protects access to the private key. Your passphrase should be at least 8 characters long and contain both letters and numbers. Punctuation characters can also be used.
File Name:
mykey
Comment:
for connecting to my_host
Passphrase:
Passphrase:
< Back
Next >
Cancel
Help

Figure 3.8: Entering a passphrase for a newly generated key pair.

Comment

In the Comment field you can write a short comment that describes the key pair - you can for example

describe the connection the files are used for. This field is not obligatory, but can be quite useful.

Passphrase

Type a phrase that you have to enter when handling the key. This passphrase works in a similar way to a password and gives some protection for your private key.

Make the passphrase difficult to guess. Use at least 8 characters, both letters and numbers. Any punctuation characters can be used as well.

Memorize the passphrase carefully, and do not write it down.

Passphrase

Type the passphrase again. This ensures that you have not made a typing error.

When you have typed in at least the file name and the passphrase (twice), you can click the Next button to proceed to the next phase.

3.3.6 Key Generation - Finish

The Key Generation - Finish page displays important information on the use of the key files.

The new public and private keys have been generated. They are currently stored on your local computer. To use these keys for public-key authentication, you have to upload the public keys to the remote host computer.

If you are connected to a remote host, you can automatically have a copy of your new public key uploaded to the server by clicking on the **Upload Public Key** button. The public key file can be uploaded at a later date as detailed in the 3.5 (Uploading Your Public Key) section.

Click the **Finish** button to exit the key generation wizard.

3.4 Connecting to a Remote Host Computer

To connect to a remote host computer, click the Connect icon on the toolbar, select the **Connect** option from the File menu, or just hit `Enter` or `Space` on the keyboard when the (still disconnected) client window is active. This brings up the **Connect to Remote Host** dialog.

When you connect to a remote host computer for the first time, the host will provide your local computer with a host public key. The host key is the public key for identifying the remote host computer that you're connecting to.

This process will bring up the Host Identification dialog.

 © 2002 SSH Communications Security Corp.

Key Generation - Finish
The public key and the private key have been generated and stored to the local disk.
To use the generated keys for public key authentication, the public key has to be uploaded to the remote host computer. If the connection is established to the remote host, upload the public key now.
Upload Public key
The public key can be also uploaded later from User Authentication - Keys page of the Global Settings dialog.
< Back
Finish
Cancel
Help

Figure 3.9: Keys have now been generated.

3.4.1 Host Identification Dialog

When you connect to a remote host computer for the first time using public-key authentication, the host sends your local computer its public key in order to identify itself. This first connection is very important.

To help you to verify the host's identity, the **Host Identification** dialog displays a fingerprint of the host's public key. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable series of five lowercase letters separated by dashes.

The fingerprint of the public key should be verified before you save it to the local database and proceed with the connection. If you do not verify the authenticity of the fingerprint, you risk the possibility of a man-in-the-middle attack. For future connections, the local copy of the server's public key will be used in server authentication.

If you have reason to suspect that the public key you have received may be forged, you can for example phone the system administrator of the remote host computer and check if the fingerprint is correct.

If your work requires the strictest degree of absolute security and you cannot trust the network that was used to deliver the host key, you can ask the system administrator of the remote host computer to deliver the host's public key to you personally, for example on a diskette. This way the key is never passed over the network and you can be absolutely sure that it has not been forged. When using that host key with an SSH Secure Shell connection, you can be sure that you are connecting to the correct host and that there is no possibility of outside intrusion. However, for ordinary use this procedure can be seen as overkill.

The **Host Identification** dialog asks if you want to store the host key on your local computer. If you connect regularly to the host you will probably want to keep the key. This prevents an attack where someone can steal your connection.

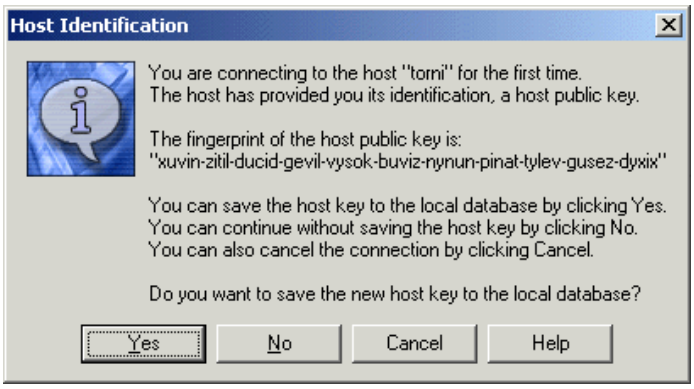
Host Identification
You are connecting to the host "torni" for the first time.
The host has provided you its identification, a host public key.
The fingerprint of the host public key is:
"xuvin-zitil-ducid-gevil-vysok-buviz-nynun-pinat-tylev-gusez-dyxix"
You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.
Do you want to save the new host key to the local database?
Yes
No
Cancel
Help

Figure 3.10: The Host Identification dialog.

Yes

You can save the host key to the local database by clicking Yes.

No

You can continue without saving the host key by clicking No. If you choose not to save the host key locally, you will be asked to the make this selection again next time you connect to this host.

Cancel

You can also cancel the connection by clicking on the Cancel button. This causes an authentication failure, and the connection will be canceled.

Help

Click the Help button to view the online help.

If you save the host key, you do not have to go through this procedure again the next time you login. The host's public key will still be checked with each connection, but this will be done automatically, without user intervention.

The known host keys will be saved in a local database that is specific to each user of the local computer. This way each user will build a personal database of the public keys of known and trusted hosts.

3.4.2 Connect to Remote Host Dialog

The **Connect to Remote Host** dialog allows you to specify the host name (or IP address), user name, port number and authentication method for the new connection.

The client remembers your previous connection. If you are going to reconnect to the same host, you do not have to type in all of the same information all over again.

 © 2002 SSH Communications Security Corp.

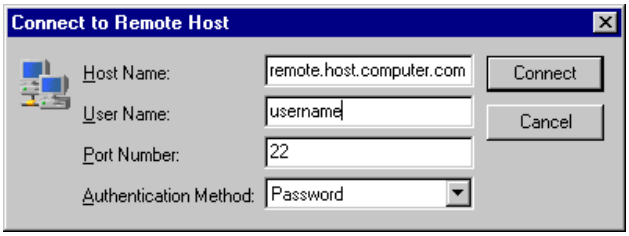

Figure 3.11: Identify yourself to the remote host computer.

Host Name

Enter the name (or IP address) of the remote host computer in this field. Unless this is your first connection, the Host Name field shows the name used in the previous connection. If you want to connect to the same computer as previously, you do not have to edit this field.

User Name

Enter your user name as used in the remote host computer. Unless this is your first connection, the User Name field shows the name used in the previous connection. If you want to connect using the same user name as previously, you do not have to edit this field.

Port Number

Type the number of the port used in the connection in the Port Number field. The standard port for Secure Shell connections is 22. The port used in the previous connection is already filled in.

Authentication Method

Select the desired authentication method from the pulldown menu. Possible authentication methods are Password, Public Key, SecurID, PAM, Keyboard Interactive and <Profile Settings>.

Password

When you login using password authentication, you will have to type your password each time you establish a new connection to the remote host computer.

Public Key

Public-key authentication is based on the use of digital signatures. If you want to use public-key authentication, first you will need to create a pair of 'key' files (see section 3.3 (Key Generation)).

Before you can login using public-key authentication, you have to upload your public key to the remote host computer (see section 3.5 (Uploading Your Public Key)).

For more information on the use of public keys, see section 3.6 (Using Public-Key Authentication).

If you are using the Secure Shell protocol version 1 (SSH1) and want to authenticate using public keys, see the SSH Secure Shell FAQ (`http://www.ssh.com/faq/`) for more information.

SecurID

Using SecurID authentication requires that you have a SecurID device that generates the numeric codes that are needed to login.

PAM

The Pluggable Authentication Modules (PAM) is an authentication method that has gained wide popularity especially on UNIX platforms.

Keyboard-Interactive

Keyboard-Interactive is designed to allow the Secure Shell client to support several different types of authentication methods. For more information on Keyboard-Interactive, see Section 8.4 (Keyboard-Interactive Authentication).

<Profile Settings>

The authentication method specified in the active profile is used. The profile-specific authentication method can be defined using the Connection page of the Settings dialog (see section 2.3.1 (Connection)).

Connect

Click the Connect button to connect to the remote host computer.

Cancel

Click the Cancel button if you change your mind and want to abort the connection.

3.5 Uploading Your Public Key

If you want to use public-key authentication when connecting to the remote host computer, you have to upload your public key to the host. If you have not yet generated your own public key, see section 3.3 (Key Generation).

Public keys can be uploaded automatically to a server. After a connection has been made to the server, a key pair can be selected from the **Keys** page of the **Settings** dialog - see 2.4.6 (Keys). Click the **Upload** button to display the **Upload Public Key** dialog that allows you to automatically upload the public key to the specified directory and automatically add an entry for the key to the `authorization` file.

Note: The automatical key uploading process will use the SFTP protocol. The administrator of the remote host computer may have restricted the user access so that users are not able to configure public-key authentication for themselves even if public-key authentication is allowed in the server configuration. If you do not have the proper file permissions to the key directory, the automatic upload will fail.

Even if the automatic upload succeeds, it may be that the server administrator has configured the system to store keys elsewhere than in the default `.ssh2` directory. In this case the keys and the authorization file additions have to be moved manually in the proper directory.

If you do not use the automatic upload facility, you will need to place your public key file in the `.ssh2` subdirectory in your home directory on the remote host computer. The default location for UNIX servers is `$HOME/.ssh2` and for Windows servers the `.ssh2` directory under the user profile directory. The `authorization` file residing in the `.ssh2` directory must be edited to take the newly transferred key into use.

Destination Folder

This is the subdirectory on the server where the public key file will be uploaded to. If this directory does not exist then it will be created under your home directory on the server (for example

 © 2002 SSH Communications Security Corp.

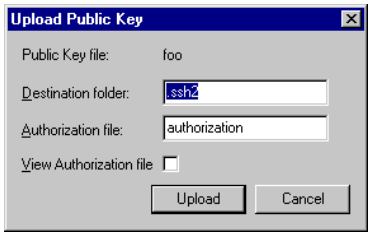

Figure 3.12: The Upload Public Key dialog.

`/home/username/.ssh2/` or `C:\Documents and Settings\username\.ssh2\`). The default value is `.ssh2`

Authorization File

This is the file on the server that contains details of your public keys. If this file does not exist then it will be created. The default value is `authorization`.

View Authorization File

Checking this box will allow you to view and edit the `authorization` file before it is uploaded to the server.

3.5.1 Manually Copying the Key File

The easiest way to manually copy your public key file is to open the **Profile Settings** page of the **Settings** dialog (select the **Settings** option from the **Edit** menu) and to click the **Browse** button next to the **User Settings Folder** field.

The folder containing your user settings is opened. The folder contains a subfolder called `UserKeys`. Double-click on the `UserKeys` folder to open it.

The folder containing your user keys is opened. Select the file that contains the public key that you want to copy to the remote host computer. Note that the public key has the file extension `.pub`. Be careful that you copy the file with the `.pub` extension, and not a similarly named file without a file extension (which would be your private key that you have to keep secure)!

Copy the file to the Windows clipboard by pressing `Control+C` on the keyboard, or by clicking the file icon with the right mouse button and selecting **Copy** from the shortcut menu.

Now connect to the remote host server and open a file transfer window, as described in Chapter 5 (File Transfer).

Your home directory should contain a subdirectory named `.ssh2`. If you do not see the `.ssh2` directory, check that you have the **Show Hidden Files** option selected from the **View** menu.

Enter the .ssh2 directory and copy the key file there from the clipboard (press `Control+V` on the keyboard or click the right mouse button and select **Paste** from the shortcut menu).

3.5.2 Manually Editing the Authorization File

The authorization file can be edited either locally on your own computer and then transferred to the remote host computer, or directly on the remote host.

Editing the `authorization` file locally

Create a plain text file called `authorization` on the your local computer (for example by using *Notepad*).

When in the text editor, add a new line containing the word `key`, a space and the file name of the public key. For example, if the public key file name is `id_dsa_1024_a.pub`, add the following line to the authorization file:

```
key id_dsa_1024_a.pub
```

(Substitute your public key filename for `id_dsa_1024_a.pub`.) If you have multiple keypairs which you use to authenticate, put each on a separate line:

```
key pub_key_one.pub
key pub_key_two.pub
```

Make sure to save the file as `"authorization"` (to omit the default file extension `.txt`, enclose the file name in quotation marks) and exit the text editor.

Then upload the `authorization` file to the `~/.ssh2` directory (or, in case of a Windows Server, in the `.ssh2` directory located under your user profile directory).

Editing the `authorization` file on a UNIX server

Alternatively you can edit the `authorization` file remotely on a UNIX server. Connect to the host using the SSH Secure Shell client's terminal window. Your home directory should contain the `.ssh2` subdirectory (note that the first character of the folder name is a full stop).

First make sure that your current directory is your home directory. Type the following command after the remote host computer command prompt and press the `Enter` key:

```
cd
```

Then enter the `.ssh2` subdirectory by issuing the following command after the command prompt:

```
cd .ssh2
```

 © 2002 SSH Communications Security Corp.

The `.ssh2` directory should contain a text file called `authorization`. You have to edit that file and add your public key file name on a separate line in that file. If the authorization file does not yet exist, you will create it now.

Start your favorite text editor by typing authorization as a parameter after the name of the text editor. For example, if your favorite text editor is *Pico*, type the following after the remote host computer's command prompt:

```
pico authorization
```

When in the text editor, add a new line containing the word `key`, a space and the file name of the public key. For example, if the public key file name is `id_dsa_1024_a.pub`, add the following line to the authorization file:

```
key id_dsa_1024_a.pub
```

Now save the authorization file and exit the text editor.

When you login the next time, public-key authentication should be working. If it does not work, check that you have typed the public key file name correctly in the `authorization` file, and that the correct public key file is located in the `.ssh2` directory on the remote host computer. Also if you connected using the **Quick Connect** option, check that you have "Public Key" selected as the authentication method.

3.6 Using Public-Key Authentication

When you connect to a remote host computer using public-key authentication, you will first see the **Connect to Remote Host** dialog. When you hit the `Enter` key, public-key authentication will be attempted and if that fails the client will try password authentication.

If there is a suitable public key, the **Enter Passphrase for Private Key** dialog should be shown. This dialog indicates that the remote host computer is willing to accept your public key to authenticate you. If you do not see the **Enter Passphrase for Private Key** dialog, check that you have properly uploaded your public key, as described in section 3.5 (Uploading Your Public Key).

Type in the passphrase associated with this key. You defined the passphrase when you create the public key - see section 3.3.5 (Key Generation - Enter Passphrase) for more information.

(If you again just press the `Enter` key, the key will not be used and the system will ask your password instead.)

If you enter the correct passphrase, you will connect to the remote host computer.

Note: In some cases the remote host computer may be configured to use both public-key authentication and some other type of authentication for increased security. In that case you may first have to authenticate yourself by some other method, and only then to use also public-key authentication.

3.7 Command Line Options

For some purposes it may be useful to operate the SSH Secure Shell for Workstations Windows Client from the command line (command prompt).

The command line syntax for SSH Secure Shell for Workstations Windows client () is the following:

```
sshclient [-r] [-p port] [-u user] [-h host] [profile.ssh2]
```

The meaning of the command line parameters is the following:

-r

The -r option will reset all customizations made to the user interface (toolbars and menus). A confirmation dialog will be displayed.

-p [port_number]

The -p option specifies the port number used for the connection. If this option is not specified, the port number defined in the default profile will be used.

-u [user_name]

The -u option specifies the user name for the connection. If this option is not specified, the user name defined in the default profile will be used.

-h [host_name]

The -h option specifies the host name for the connection. If this option is not specified, the host name defined in the default profile will be used.

[profile.ssh2]

If a profile is specified, it must the last option on the command line. Any command line parameters will override the profile settings. If no profile is specified, the default profile (`default.ssh2`) will be used.

For example, the following command would immediately start a connection to a host called remotehost and connect as guest. The port number is not specified, so the connection would use the port specified in the default profile.

```
sshclient -h remotehost -u guest
```

The following command would immediately start a connection to remotehost using the settings defined in the profile file `custom.ssh2`.

```
sshclient -h remotehost custom.ssh2
```

 © 2002 SSH Communications Security Corp.

If the host is not specified (using the -h option) and no profile is specified, the login dialog will open, automatically filled with the values specified on the command line.

For example, the following command would display the login dialog with the port number already defined as 222 and the user name as guest.

```
sshclient -u guest -p 222
```

Note: A pure command line version of the SSH Secure Shell client is shipped with the Windows client. The command line client `SSH2.EXE` is a port of the UNIX version of SSH Secure Shell, and may be useful also in the Windows command line environment, especially for when creating scripts. For a more detailed description of the `SSH2.EXE` syntax, see Appendix A.1 (SSH.EXE).

Also several other command line utilities are shipped with the Windows and command line clients. For more information, see the appendices section (A (Appendices)).

Chapter 4

Terminal Window

The terminal window is a secure replacement for Telnet connections. It offers a command line interface to the remote host computer. Note that the most important function of the terminal window is to allow you to operate the remote host computer. Therefore the terminal window does not capture some common keyboard shortcuts (such as `Ctrl+C` for copy), but passes them instead to the remote host computer, where they can be used to control remote program execution.

Apart from the text display itself, a lot of connection information is visible in title and status bars of the Terminal window.

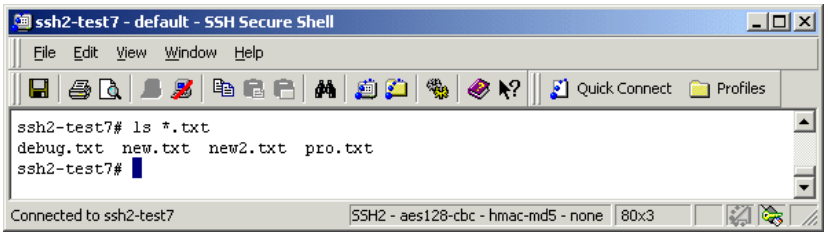

Figure 4.1: The Terminal window.

4.1 Terminal Window Title Bar

The title bar is located on the top of the window.

The leftmost item on the title bar is the window icon. Click it to display the Window menu or doubleclick it to close the window.

The next item on the title bar is the window's sequence number. This helps you to distinguish between different windows using the same connection.

 © 2002 SSH Communications Security Corp.

Next on the title bar is displayed the remote computer's host name. For example, a second window associated with a connection to a host computer called 'remote' would display as `2:remote`.

After the host name, the next item on the title bar is the name of the settings file in use. If you are not using a settings file that has been saved with a specific file name (using the **Save As** option on the **File** menu), a settings file called `default` is in use.

If you have changed the settings without saving them, an asterisk (`*`) is displayed on the title bar, after the name of the current settings file (for example: `default*`). For information on saving the changed settings, see Section 2.1 (Saving Settings).

The last text item on the title bar is the name of the client, `SSH Secure Shell`.

4.2 Terminal Window Status Bar

The status bar is located at the bottom of the Terminal window. When browsing through the menu options or toolbar buttons, the status bar displays a short context sensitive help text.

When the menus or toolbars are not browsed, the left side of the status bar indicates to which remote host computer you are currently connected. If you are not connected, the status bar displays the text `Not connected - Press Enter/Space to connect`.

The next status bar field shows the current protocol version, encryption algorithm, and MAC algorithm separated by dashes (for example: `ssh2 - 3des-cbc - hmac-md5`). Note that the status bar displays some of the algorithm names in a longer form than the Connection screen of the Settings dialog.

The next field displays the number of columns and rows of the terminal window. If you change the size of the terminal window, this window size indicator will be immediately updated.

If you are connecting through a firewall, the next field of the status bar displays a firewall icon when the firewall is in use. Click the firewall field to open the **Firewall** page of the **Settings** dialog. For more information, see the section 2.4.21 (Firewall).

The next field displays the SSH Accession icon. If SSH Accession is running, the icon is displayed normally, otherwise it is grayed out. Click the SSH Accession field to open the **SSH Accession** page of the **Settings** dialog. For more information, see the section 2.4.9 (SSH Accession).

If you have a smart card reader active, you should see a small card reader icon on the next column of the status bar. When a token is inserted, a smart card appears in the card reader in the icon. When a key is acquired from the token, a key symbol appears on top of the card reader icon. Click the smart card reader field to open the **PKCS #11** page of the **Settings** dialog. For more information, see the section 2.4.10 (PKCS 11). If the smart card reader icon does not appear, see section 2.4.12 (PKCS 11 Provider) for troubleshooting information.

The next field displays the text `CAP` if your Caps Lock key is currently on.

The last field of the terminal window status bar displays the text NUM if your Num Lock key is currently on.

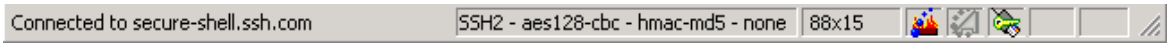

Figure 4.2: Terminal window status bar.

4.3 Terminal Window Shortcut Menu

If you have not set the **Paste on Right Mouse Click** option (see 2.4.1 (Appearance)), a shortcut menu appears when you click the terminal window with the right mouse button.

By default, the following menu options are available:

Copy

Copy text into the Windows clipboard.

Paste

Paste text from the Windows clipboard.

Paste Selection

Copy the currently selected text into the cursor location without first copying it into the Windows clipboard.

Select All

Select all of the scrollback buffer.

Select Screen

Select all text currently displayed on the screen. The rest of the scrollback buffer will not be selected.

Select None

Cancel the current selection.

Find

Search for text from the scrollback buffer.

New Terminal

Open a new terminal window.

New File Transfer

Open a new File Transfer window.

Close Window

Close the current window.

 © 2002 SSH Communications Security Corp.

Settings

Open the Settings dialog.

The available options can be configured using the **Customize** dialog (see section 2.5 (Customize)).

Chapter 5

File Transfer

SSH Secure Shell makes it easy and convenient to transfer files between your local computer and the remote host computer (server). You can upload and download files by using an intuitive, graphical user interface similar in functionality to *Windows Explorer*.

You can open the **File Transfer** window by clicking on the **New File Transfer Window** button on the SSH Secure Shell toolbar, or by selecting the **New File Transfer** option (or the **New File Transfer in the Current Directory** option) from the **Window** menu. You can have an unlimited number of individual **File Transfer** windows open at the same time.

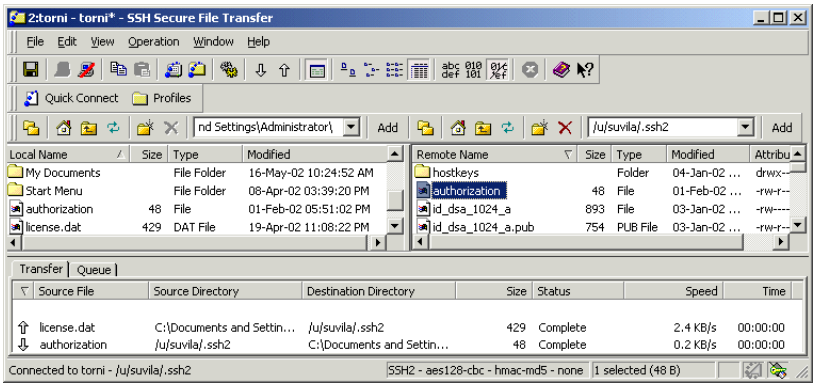
2:torni - torni* - SSH Secure File Transfer
File Edit View Operation Window Help
Quick Connect Profiles
nd Settings\Administrator\ Add
/u/suvila/.ssh2 Add
Local Name Size Type Modified
My Documents File Folder 16-May-02 10:24:52 AM
Start Menu File Folder 08-Apr-02 03:39:20 PM
authorization 48 File 01-Feb-02 05:51:02 PM
license.dat 429 DAT File 19-Apr-02 11:08:22 PM
Remote Name Size Type Modified Attribu
hostkeys Folder 04-Jan-02 ... drwx--
authorization 48 File 01-Feb-02 ... -rw-r--
id_dsa_1024_a 893 File 03-Jan-02 ... -rw----
id_dsa_1024_a.pub 754 PUB File 03-Jan-02 ... -rw-r--
Transfer Queue
Source File Source Directory Destination Directory Size Status Speed Time
license.dat C:\Documents and Settin... /u/suvila/.ssh2 429 Complete 2.4 KB/s 00:00:00
authorization /u/suvila/.ssh2 C:\Documents and Settin... 48 Complete 0.2 KB/s 00:00:00
Connected to torni - /u/suvila/.ssh2
SSH2 - aes128-cbc - hmac-md5 - none
1 selected (48 B)

Figure 5.1: The File Transfer window.

SSH Secure Shell File Transfer contains several unique features that make secure transfer operations fast and easy. Note, however, that the SSH Secure Shell for Workstations Windows client is not just an alternative to an FTP client. You cannot for example use the Secure Shell client to login to a normal, insecure FTP server. The remote host computer must be running SSH server software.

 © 2002 SSH Communications Security Corp.

5.1 File Transfer Window Layout

The **File Transfer** window works a lot like *Windows Explorer*: it displays the contents of any open directories represented as icons and optionally gives basic information (such as size and type) on each file.

The File Transfer windows consists of three panes: **Local View** (displaying the files on your local computer), **Remote View** (displaying files on the server) and **Transfer View** (displaying files transferred between the local and remote computers).

By default, **Local View** is displayed on the left-hand side of the window, **Remote View** on right-hand side of the window, and **Transfer View** below the **Local** and **Remote Views**. You can change the default layout on the **File Transfer** page on the **Global Settings** section of the **Settings** dialog - for more information, see section 2.4.17 (File Transfer).

5.1.1 File Transfer Title Bar

The title bar is located on the top of the **File Transfer** window.

The leftmost item on the title bar is the window icon. Click it to display the Window menu or doubleclick to close the window.

The next item on the title bar is the window's sequence number. This helps you to distinguish between different windows using the same connection.

Next on the title bar is displayed the remote computer's host name. For example, a second window associated with a connection to a host computer called 'remote' would display as `2:remote`.

After the host name, the next item on the title bar is the name of the settings file in use. If you are not using a settings file that has been saved with a specific file name (using the **Profiles** option), a settings file called `default` is in use.

If you have changed the settings without saving them, an asterisk (`*`) is displayed on the title bar, after the name of the current settings file (for example: `default*`). For information on saving the changed settings, see Section 2.1 (Saving Settings).

The last text item on the title bar is the name of the client, `SSH Secure Shell File Transfer`.

5.1.2 File Transfer Menu Bar

Under the **File Transfer** window's title bar lies the menu bar. Most of the menu options are the same as in the terminal window, but the **Operation** menu is unique to the **File Transfer** window, and some file transfer specific options have been added to the **View** menu, and some terminal windows specific options have been removed from the **Edit** menu. The File Transfer window's menu options are detailed in Chapter 7 (Menu Reference).

The position and contents of the menu bar can be freely customized - see sections 7.1.1 (Moving Menus) and 2.5 (Customize).

5.1.3 File Transfer Toolbars

Three individual toolbars are available in the **File Transfer** window, all of them initially located below the menu bar:

Toolbar

The basic toolbar that is displayed also in the terminal window, augmented for some file transfer specific toolbar buttons. For more information, see Chapter 6 (Toolbar Reference).

Profile Bar

A separate toolbar for managing the server profiles and the **Quick Connect** option. For more information, see section 6.17 (Profile Bar).

File Bar

A separate toolbar for the most commonly used file management tasks. For more information, see section 6.18 (File Bar).

The layout and contents of the tool bar and the profile bar can be freely customized - see sections 6.1 (Configuring Toolbars) and 2.5 (Customize). The file bar is a dynamically created toolbar, and therefore it cannot be customized.

5.1.4 File Transfer Status Bar

The status bar is located at the bottom of the **File Transfer** window. When browsing through the menu options or toolbar buttons, the status bar displays a short context sensitive help text on the currently active user interface element (such as toolbar button or menu item).

When the menus or toolbars are not browsed, the left side of the status bar displays the current remote host computer (server) and the current directory on the remote host.

Figure 5.2: The File Transfer status bar displaying the size of a selected file.

The next status bar field shows the current protocol version, encryption algorithm, and MAC algorithm separated by dashes (for example: `ssh2 - 3des-cbc - hmac-md5`). Note that the status bar displays some of the algorithm names in a longer form than the Connection screen of the Settings dialog.

The next field of the File Transfer status bar displays the number of files and subfolders in the current folder, as well as the total size of the files. If you select file(s) in the folder view, the field changes to display the

 © 2002 SSH Communications Security Corp.

number and total file size of the current selection. This is especially useful when estimating the amount of total data to be transferred.

If you are connecting through a firewall, the next field of the status bar displays a firewall icon when the firewall is in use. Click the firewall field to open the **Firewall** page of the **Settings** dialog. For more information, see the section 2.4.21 (Firewall).

The next field displays the SSH Accession icon. If SSH Accession is running, the icon is displayed normally, otherwise it is grayed out. Click the SSH Accession field to open the **SSH Accession** page of the **Settings** dialog. For more information, see the section 2.4.9 (SSH Accession).

If you have a smart card reader active, you should see a small card reader icon in the last field of the status bar. When a token is inserted, a smart card appears in the card reader in the icon. When a key is acquired from the token, a key symbol appears on top of the card reader icon. Click the smart card reader field to open the **PKCS 11** page of the **Settings** dialog. For more information, see section 2.4.10 (PKCS 11). If the smart card reader icon does not appear, see section 2.4.12 (PKCS 11 Provider) for troubleshooting information.

5.1.5 Contents of the File Transfer Window

Local and **Remote Views** can display their contents in four different ways, as defined in the global **File Transfer** page of the **Settings** dialog - see 2.4.17 (File Transfer). The available views are the following:

Large Icons

Each file and folder has a large icon associated with it, making for a clear and uncluttered display. The only information displayed about each file is the icon and the file name.

Small Icons

Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view. No more information than the icon and the name of each file is displayed.

List

Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other. Only the icons and the file names are displayed.

Details

The files and folders are displayed with a small icon, their file name, file size, file type, their last modification date. The files in the Remote View have also their attributes visible. This is the default view.

By clicking on the **Name**, **Size**, **Type**, **Modified** or **Attributes** sort bars located on top of the directory listing, you can sort the files and folders based on their file name, file size, file type, the time they were last modified, and file attributes. Clicking the same sort option again reverses the sorting order.

Note: The sort function is not case sensitive - upper case text is sorted together with lower case text.

The following information is displayed in each column:

Name

The file name of each file. Note that the local and remote file systems limit what file names are acceptable on which computer. (For example, UNIX file names are case sensitive while Windows file names are not. Thus a UNIX directory may contain both `File.txt` and `file.txt`, but a Windows directory may not.)

Size

The size of each file, expressed in bytes.

Type

The type of each file is based on the file extension. The descpription given in the Type field is based on the file types recognized by *Windows Explorer*. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the remote computer.

Modified

The last time when each particular file has been changed.

Attributes

The attributes of each file.

On Windows systems, the file may have the following attributes:

R
The file can be read.

W
The file can be written to.

X
The file can be executed (run).

On UNIX systems, the attributes signify the file permissions given to each file:

d
The entry is a directory.

r
The file can be read.

w
The file can be written to.

x
The file can be executed.

After the `d` attribute, the `r w` and `x` attributes may be repeated up to three times. If the file does not have a particular attribute, the attribute is replaced with a hyphen (`-`).

The first three attributes specify the permissions given to the owner of the file, the second triplet specifies the permissions for the user group associated with the file, and the last triplet specifies the permissions given to all other users. For more information on file permissions, please consult the server's documentation.

 © 2002 SSH Communications Security Corp.

5.1.6 Local View

The contents of current directory on your local computer are visible on the **Local View** of the **File Transfer** window. By default, **Local View** displays the contents of your local home directory - usually your Windows desktop. You can change the home directory on the **Local Favorites** page of the **Settings** dialog - see section 2.4.20 (Local Favorites).

5.1.7 Local Folder View

Local View can optionally contain a separate window pane for the local directory structure. By default, the **Local Folder View** pane is hidden. You can show and hide it again by clicking the **Show/Hide Local Folders** button on the File bar.

The directory structure is presented as a tree-like folder structure, familiar from *Windows Explorer*. Folders that have a plus sign (+) next to them can be opened by clicking on the plus sign. Open folders have a minus sign (-) next to them and can be closed by clicking on the minus sign.

You can click on a folder to view its contents on the right hand side pane of **Local View**. The displayed folder shows up highlighted in the folder view.

Just opening or closing a folder in the folder view does not affect the file view on the right hand side, unless you close the displayed folder's parent folder. In that case the closed folder becomes the new displayed folder.

5.1.8 Remote View

The contents of current directory on the remote host computer (server) are visible on the **Remote View** of the **File Transfer** window. By default, **Remote View** displays the contents of your home directory on the remote host computer. You can change the default directory on the **Remote Favorites** page of the **Settings** dialog - see section 2.3.9 (Remote Favorites).

5.1.9 Remote Folder View

Remote View can optionally contain a separate window pane for the remote directory structure. By default, the **Remote Folder View** pane is hidden. You can show and hide it again by clicking the **Show/Hide Remote Folders** button on the File bar.

The directory structure is presented as a tree-like folder structure, familiar from *Windows Explorer*. Folders that have a plus sign (+) next to them can be opened by clicking on the plus sign. Open folders have a minus sign (-) next to them and can be closed by clicking on the minus sign.

You can click on a folder to view its contents on the right hand side pane of **Remote View**. The displayed folder shows up highlighted in the folder view.

Just opening or closing a folder in the folder view does not affect the file view on the right hand side, unless you close the displayed folder's parent folder. In that case the closed folder becomes the new displayed folder.

5.1.10 Transfer View

The file transfer operations between the local and the remote host computer are displayed on the **File Transfer** window's **Transfer View**. **Transfer View** consists of the **Transfer** page and the **Queue** page. Click the appropriate tab on top of **Transfer View** to change between the pages.

Transfer Page

The **Transfer** page of **Transfer View** displays a list of files that have been transferred between the computers. The page gives the following information on the transferred files:

Direction

The direction of the transfer is depicted with an arrow icon. Uploads are marked with an arrow pointing up, and downloads with a donwwards pointing arrow.

Source File

The original name of the file in the source system.

Source Directory

The directory where the file was transferred from.

Destination Directory

The directory where the file was transferred to.

Size

The size of the file, expressed in bytes.

Status

The transfer status of the file. Files waiting for the transfer to start are marked as `Queued`. The status of ongoing transfers is displayed as a progress bar. Successfully transferred files are marked as `Complete`. Files whose transfer operation has been cancelled, are marked as `Cancelled`. Errors that prevent the file transfer from completing are displayed in the status column as well.

Speed

The speed of the transfer operation, expressed in kilobytes per second.

Time

During the transfer operation the Time column displays the estimated time to complete the transfer. After the transfer has been completed, the actual time used for the transfer is displayed.

 © 2002 SSH Communications Security Corp.

To stop transferring files, select the files that you do not want to be transferred, right-click the Transfer page and then select the **Cancel** option from the shortcut menu.

To delete files from the queue, select the files that you do not want to keep in the Transfer page, right-click the Transfer page and then select the **Remove** option from the shortcut menu.

To transfer again files that were not succesfully transferred previously, select the files, right-click the Transfer page and then select the **Retry** option from the shortcut menu.

To remove files from the local directory, select the files that you do not want to keep in the local directory, right-click the Transfer page and then select the **Delete Local File** option from the shortcut menu.

To remove files from the remote directory, select the files that you do not want to keep in the remote directory, right-click the Transfer page and then select the **Delete Remote File** option from the shortcut menu.

To remove completely transferred and cancelled files from the Transfer page, right-click the Transfer page and then select the **Clear Finished** option from the shortcut menu.

To export the list into a text file, right-click the Transfer page and then select the **Export List** option from the shortcut menu. The **Save As** dialog appears, allowing you to specify the location and name of the text file. The text file will contain the path and file names of the transferred files in both the remote and local system, and the file size, separated by commas. This option can be used to maintain a log of your file transfers.

Queue Page

The **Queue** page of **Transfer View** can be used to create a customized list of files that are to be transferred at a later stage. You can use the mouse to drag and drop files on the Queue page, where they then wait to be transferred.

Alternatively you can right-click on the Queue page and select the **Add** option from the shortcut menu to add more files to the queue. The **Edit Transfer Queue** dialog appears. Then click the **New** button above the list area to type in the path to a new file to be transferred, or click the ellipsis button (`...`) to open a file selector dialog.

To edit the target locations of the queued files, select a file to edit, right-click the Queue page and choose **Edit** from the shortcut menu. The **Edit Transfer Queue** dialog appears, allowing you to type in a new destination directory for the file. You can also click the ellipsis button (`...`) to open a file selector dialog that you can use to select the destination directory.

You can use the **Edit** option for several files at the same time, but the direction of the transfer (upload or download) must be the same for all of the files.

To delete files from the queue, select the unwanted files, right-click the Queue page and choose **Remove** from the shortcut menu.

To transfer single files, select them, right-click the Queue page and choose **Transfer** from the shortcut menu.

To transfer all the queued files, right-click the Queue page and choose **Transfer All** from the shortcut menu.

5.2 Navigating in the File Transfer Window

You can change the current directory in the Local or the Remote View by any of the following methods:

- Double-click the folders displayed in the current view to open them. (Use the **Up** button on the file bar to return to the parent directory.)

  In **Local View**, you can access other drives by clicking the **Up** button until you are on the Windows desktop directory and then double-clicking the **My Computer** icon.

- Select other drives and directories from the favorites drop-down list box displayed on the file bar. You can customize the contents of the **Local Favorites** list on the **Local Favorites** page of the **Settings** dialog (see section 2.4.20 (Local Favorites)) and the contents of the **Remote Favorites** list on the **Remote Favorites** page of the **Settings** dialog (see section 2.3.9 (Remote Favorites)).

- Type in the path to the desired directory (for example `C:\Program Files` or `./.ssh2`) in the favorites drop-down list and press the `Enter` key to move to that directory.

5.2.1 Drag And Drop Operations

You can use the mouse to drag and drop files between the local and remote computers. This works in a similar fashion to the standard Windows drag and drop operations. If you hold down the `Shift` or `Control` keys when selecting files with the mouse, you can select multiple files and copy them all at the same time. If you hold down the `Shift` key, all the files and folders between the first and last selection will be selected. If you hold down the `Control` key, you can select individual files and folders one by one.

If you doubleclick a file, the file will be opened by using a custom application. (*Notepad* will be used by default.) For more information on specifying the custom application, see section 2.4.17 (Missing File Association).

5.3 File Transfer Shortcut Menus

Click the **File Transfer** window with the right mouse button to display a shortcut menu. The available menu options vary depend on whether you click on the Local or the Remote View and whether you have selected a file or not.

 © 2002 SSH Communications Security Corp.

5.3.1 Local View

The following shortcut menu options are available in **Local View** when you have not selected a file or a folder:

Up

Move the File Transfer window focus into the parent directory of the current directory.

Home

Move the File Transfer window focus into your home directory.

Refresh

Redraw the File Transfer window.

Select All

Select all files and folders in the current folder. The shortcut key for Select All is `Ctrl+A`.

View

Opens a submenu from which you can select the view type (large icons, small icons, list or details view).

New Folder

Creates a new folder and prompts you to enter a name for it. If you enter nothing, the folder will not be created.

The following shortcut menu options are available in **Local View** when you have selected a file or a folder:

Open

Open the currently selected file or folder. The shortcut key for Open is `Ctrl+O`.

Upload

Transfer a file from the local computer into the remote host computer.

Delete

Remove the currently selected file.

Rename

Change the name of the currently selected file. The shortcut key for Rename is `F2`.

Properties

Display the attributes of the currently selected file, including the file permissions (on UNIX systems).

5.3.2 Remote View

The following shortcut menu options are available in **Remote View** when you have not selected a file or a folder:

Up

Move the File Transfer window focus into the parent directory of the current directory.

Home

Move the File Transfer window focus into your home directory. The shortcut key for Home is `Ctrl+H`.

Go to Folder

Opens the **Go to Remote Folder** dialog where you can type in a path of the folder which you want to open.

Refresh

Redraw the File Transfer window. The shortcut key for Refresh is `F5`.

Select All

Select all files and folders in the current folder. The shortcut key for Select All is `Ctrl+A`.

Paste

Paste a file from the File Transfer 'clipboard'. The shortcut key for Paste is `Ctrl+V`.

Upload Dialog

Opens the **Upload - Select Files** dialog that allows you to select a file and transfer it from the local computer into the remote host computer. The shortcut key for Upload Dialog is `Ctrl+U`.

View

Opens a submenu from which you can select the view type (large icons, small icons, list or details view).

Arrange Icons

Opens a submenu from which you can select how the icons are arranged (by name, by type, by size or by date).

New Folder

Creates a new folder and prompts you to enter a name for it. If you enter nothing, no folder will be created. The shortcut key for New Folder is `Ctrl+N`.

The following shortcut menu options are available in **Remote View** when you have selected a file or a folder:

Open

Open the currently selected file or folder. The shortcut key for Open is `Ctrl+O`.

 © 2002 SSH Communications Security Corp.

Download

Transfer the currently selected file into the local computer.

Download Dialog

Open the **Download - Select Folder** dialog that allows you to select a folder on the local computer and transfer the currently selected file into it. The shortcut key for Download Dialog is `Ctrl+D`.

Copy

Copy the currently selected file into the File Transfer 'clipboard'. The shortcut key for Copy is `Ctrl+C`.

Delete

Remove the currently selected file.

Rename

Change the name of the currently selected file. The shortcut key for Rename is `F2`.

Properties

Display the attributes of the currently selected file, including the file permissions (on UNIX systems).

The available shortcut menu options can be configured using the Customize dialog (see section 2.5 (Customize)).

5.3.3 Transfer Page

The following shortcut menu options are available on the **Transfer Page** of the **Transfer View**:

Cancel

To stop transferring the files, select the files that you do not want to be transferred, right-click the Transfer page and then select the **Cancel** option from the shortcut menu.

Remove

To delete files from the queue, select the files that you do not want to keep in the Transfer page, right-click the Transfer page and then select the **Remove** option from the shortcut menu.

Retry

To transfer again files that were not succesfully transferred previously, select the files, right-click the Transfer page and then select the **Retry** option from the shortcut menu.

Delete Local File

To remove files from the local directory, select the files that you do not want to keep in the local directory, right-click the Transfer page and then select the **Delete Local File** option from the shortcut menu.

Delete Remote File

To remove files from the remote directory, select the files that you do not want to keep in the remote directory, right-click the Transfer page and then select the **Delete Remote File** option from the shortcut menu.

Clear Finished

To remove completely transferred and cancelled files from the Transfer page, right-click the Transfer page and then select the **Clear Finished** option from the shortcut menu.

Export List

To export the list into a text file, right-click the Transfer page and then select the **Export List** option from the shortcut menu. The **Save As** dialog appears, allowing you to specify the location and name of the text file. The text file will contain the path and file names of the transferred files in both the remote and local system, and the file size, separated by commas. This option can be used to maintain a log of your file transfers.

5.3.4 Queue Page

The following shortcut menu options are available on the **Queue Page** of the **Transfer View**:

Transfer

To transfer single files, select them, right-click the Queue page and choose **Transfer** from the shortcut menu.

Transfer All

To transfer all the queued files, right-click the Queue page and choose **Transfer All** from the shortcut menu.

Add

To add more files to the transfer queue, right-click on the Queue page and select the **Add** option from the shortcut menu. The **Edit Transfer Queue** dialog appears. Then click the **New** button above the list area to type in the path to a new file to be transferred, or click the ellipsis button (`...`) to open a file selector dialog.

Edit

To edit the target locations of the queued files, select a file to edit, right-click the Queue page and choose **Edit** from the shortcut menu. The **Edit Transfer Queue** dialog appears, allowing you to type in a new destination directory for the file. You can also click the ellipsis button (`...`) to open a file selector dialog that you can use to select the destination directory.

You can use the **Edit** option for several files at the same time, but the direction of the transfer (upload or download) must be the same for all of the files.

Remove

To delete files from the queue, select the unwanted files, right-click the Queue page and choose **Remove** from the shortcut menu.

 © 2002 SSH Communications Security Corp.

5.4 Differences From *Windows Explorer*

The **File Transfer** window operates very much the same way as the familiar *Windows Explorer*. However, due to the different nature of handling files locally in your own computer (as per Windows Explorer) and handling them over a secured remote connection in the host computer (as per SSH Secure Shell File Transfer), there are some differences in operation.

Deleting folders

It is not possible to delete a remote folder that is not empty. Delete the files and subfolders residing in the folder first.

Multiple paste operations

During copy and paste operations, the file names are not changed when the files are pasted. Therefore it is not possible to paste files several times into one location, creating 'copies of' the pasted files as in Windows Explorer.

Note: The maximum size of transferred files is limited only by the file system. (On many systems the maximum file size is 2 gigabytes.)

5.5 Downloading Files

By using the **File Transfer** window it is easy to download files from the remote host computer into your local computer. There are several different ways to download a file - or several files at the same time.

To select multiple files, hold down the `Shift` or `Control` keys when selecting files with the mouse. If you hold down the `Shift` key, all the files and folders between the first and last selection will be selected. If you hold down the `Control` key, you can select individual files and folders one by one.

Drag and drop

Dragging and dropping is probably the easiest way to download files. Simply click on the file(s) you want to download, hold down the mouse button and move the file to a location where you want it - for example on the Windows desktop - and release the button.

Download button

You can click the **Download** button on the toolbar to download the selected file(s).

Shortcut menu

When you right-click on a file in **Remote View**, a shortcut menu appears. Select the **Download** or **Download Dialog** option from the menu.

If you have selected the **Download Dialog** option, a **Download - Select Folder** dialog will appear, allowing you to select where the downloaded file(s) should be saved. After you have selected the appropriate folder (or other location), **Transfer View** shows the current downloading status.

5.5.1 Download - Select Folder Dialog

When you start a download operation, a **Download - Select Folder** dialog is displayed. This is a standard Windows file selection dialog, where you can select the location where you want the selected file(s) to be downloaded.

You can use the **Look in** selection box to select a folder, a local or network drive or your desktop.

Note: Transferring files to or from a network drive is not supported on Windows 95.

Another way to select the desired folder is to type its directory path in the Folder field. Note that you can use this field only to specify the folder name. Do not write in a file name after the selected directory path. The file name will be the same the file has in the remote host computer.

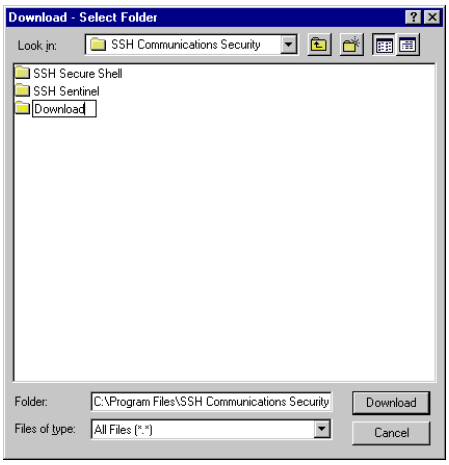

Figure 5.3: Creating a new directory for downloaded files.

The most common operations can be achieved by clicking on the four buttons on the right hand side of the **Look in** selection box. You can click on the **Up One Level** button to move to the parent folder of the current folder. If you want to create a new folder, click on the **Create New Folder** button. You can also select between the **Small Icons** and **Details** views by clicking on the appropriate buttons.

5.6 Uploading Files

The File Transfer window can be used to upload files from your local computer to the remote host computer. There are several different ways to upload a file.

It is also possible to upload several files at the same time. To select multiple files, hold down the Shift or Control keys when selecting files with the mouse. If you hold down the `Shift` key, all the files and folders between the first and last selection will be selected. If you hold down the `Control` key, you can select individual files and folders one by one.

 © 2002 SSH Communications Security Corp.

Drag and drop

Dragging and dropping is probably the easiest way to upload files. Simply click on the local file(s) you want to upload (for example on the desktop or the *Windows Explorer*), hold down the mouse button, move the file(s) into the **File Transfer** window's file view and release the button.

Upload button

You can click the **Upload** button on the **File Transfer** window's toolbar to upload the selected file(s).

Shortcut menu

When you right-click on a file in **Local View** or on an empty space in the **Remote View**, a shortcut menu appears. Select the **Upload** or **Upload Dialog** option from the menu.

If you have selected the **Upload Dialog** option, a **Upload - Select Files** dialog will appear, allowing you to select the file(s) to upload. After you have selected the files, **Transfer View** shows the current downloading status.

5.6.1 Upload - Select Files Dialog

When you start an upload operation, a **Upload - Select Files** dialog is displayed. This is a standard Window file selection dialog, where you can select which file(s) you want to upload.

You can use the **Look in** selection box to select the location of the file(s): a folder, a local or network drive or your desktop.

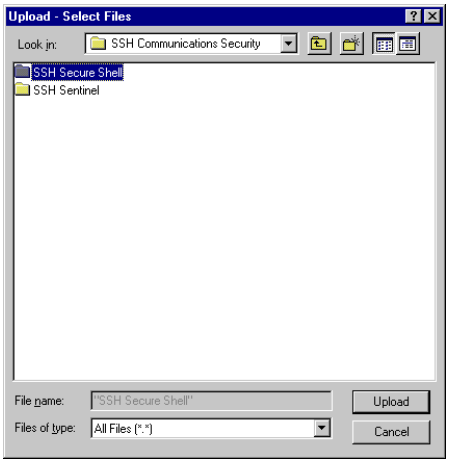

Figure 5.4: Select the file you want to upload.

Note that the grayed out File name field displayed at the bottom of the dialog displays the selected file name. The field is read-only - you cannot type in the desired file name. Select the files by clicking them with the mouse instead.

The most common operations can be achieved by clicking on the four buttons on the right hand side of the **Look in** selection box. You can click on the **Up One Level** button to move to the parent folder of the current

folder. If you want to create a new folder, click on the **Create New Folder** button. You can also select between the **Small Icons** and **Details** views by clicking on the appropriate buttons.

5.7 File Properties

Selecting a file in **Local View** or **Remote View** and then selecting the **Properties** option (from the shortcut menu or the **Operation** menu) brings up the **File Properties** dialog which allows you to view and change some of the file's properties.

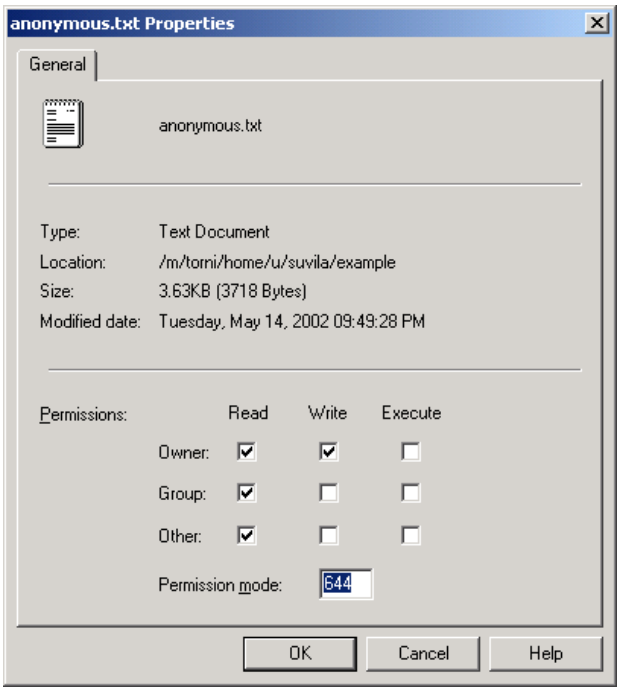

Figure 5.5: Properties page for a file.

File Name

At the top of the page the file name and icon are shown. If multiple files are selected, a count of the number of files and folders is displayed.

Type

The type of the selected file(s).

Location

The directory where the selected file(s) are located on the remote host.

Size

The size of the selected file. If multiple files are selected the total size of all the files is diplayed.

 © 2002 SSH Communications Security Corp.

Modified Date

The last modified date for the selected file.

Permissions

The **Permissions** check boxes are displayed for files residing in a UNIX system. The 9 check boxes can be used to set the permissions of a file or a group of files. If multiple files are selected with conflicting permissions then some of the check boxes will appear grayed out. Clicking on a greyed out check box will clear the check mark. If there are any check boxes are grayed out when the OK button is pressed it will have the effect of leaving that value unchanged on the remote file.

Permissions can also be set by entering standard octal UNIX permissions (as with the UNIX `chmod` command) in the **Permission mode** field. Values entered here override and update the check box values.

For more information on file permissions, see section 5.1.5 (Contents of the File Transfer Window).

Attributes

The **Attributes** check boxes are displayed for files residing in a Windows system. The 5 check boxes (Read-only, Hidden, Archive, System and Compressed) can be used to set the attributes of a local file or a local group of files. If multiple files are selected with conflicting permissions, then some of the check boxes will appear grayed out. Clicking on a greyed out check box will clear the check mark. If there are any check boxes are grayed out when the **OK** button is pressed, it will have the effect of leaving that value unchanged on the remote file.

Note: Due to the limitations of the Windows architecture, it is not possible to set the Windows file attributes for remote files residing on a Windows server.

For more information on file attributes, see section 5.1.5 (Contents of the File Transfer Window).

Chapter 6

Toolbar Reference

The most commonly used functions of SSH Secure Shell for Workstations's **Terminal** and **File Transfer** windows can be accessed using the *toolbar*. By default the basic Toolbar is located on top of the SSH Secure Shell client window, right under the menubar.

Figure 6.1: The basic Toolbar contains buttons for the most frequently used functions.

Initially the Profiles bar is located under the basic toolbar, containing the **Quick Connect** and **Profiles** options.

Figure 6.2: The Profiles bar contains the Quick Connect and Profiles buttons.

In the File Transfer window, a third toolbar is available. The default position of the File bar is below the Profiles toolbar.

Figure 6.3: The File bar is specific to the File Transfer window.

6.1 Configuring Toolbars

The SSH Secure Shell for Workstations Windows client has a dynamic user interface that is very easy to modify to match to your tastes. You can select the position of the toolbars, and even move individual buttons from one place to another.

Note: The file bar displayed in the File Transfer window is dynamically created, and therefore it cannot be customized.

 © 2002 SSH Communications Security Corp.

6.1.1 Moving Toolbars

You can use the mouse to grab the toolbars by their handles (located on the left-hand end of each toolbar) and move them around the SSH Secure Shell window.

You can have the toolbars floating freely in the window, or anchor them in the top, bottom or even either side of the window. Experiment to find the toolbar positions that you like best.

6.1.2 Moving Toolbar Buttons

You can also move individual toolbar buttons around and arrange them so that they best serve your needs.

To move a toolbar button, keep the `Alt` key on the keyboard pressed down and grab a button with your mouse. You will see a new mouse pointer appear. Click the button with your left mouse button, keep the mouse button pressed down and move the button around. When you release the mouse button, the toolbar button will be move to a new position.

Note: If you move a button to somewhere else than a toolbar (for example, in the terminal window text area), it is removed from the window. But don't worry - the changes become permanent only if you use the **Save Settings** option (see section 6.2 (Save Settings)).

6.1.3 Permanent Toolbar Changes

If you want to make the new toolbar positions permanent, use the **Save Settings** option (from the toolbar or the **File** menu) to save your settings.

If you change your mind and want to return the toolbars to their original positions, select the **Reset Toolbars** option from the **View** menu. A confirmation dialog will open, asking if you really want to discard the changes you have made. If you select **Yes**, the toolbars will return to their original configuration. If have modified your menus, this option will reset them as well.

6.2 Save Settings

Select the **Save Settings** option (from the **File** menu or the toolbar) to save any changes you have made to your current settings. The default settings file where the configuration will be saved is `default.ssh2`.

If you want to save your current settings in a new settings file, select the **Add Profile** option under the **Profiles** option (see section 3.2 (Profiles)).

6.3 Print

Select the **Print** option to output the contents of the current scrollback buffer to your printer. The standard Windows **Print** dialog will appear, allowing you to select the printer settings.

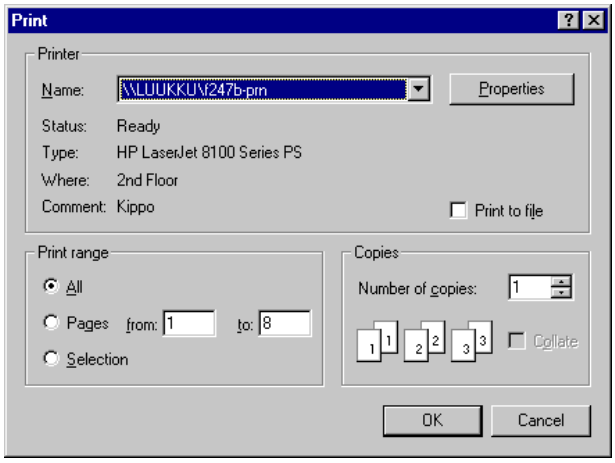

Figure 6.4: The Print dialog allows you to specify the printer settings.

The print range can also be selected from this dialog. Selecting **All** will print the entire contents of the terminal scrollback buffer. If the whole scrollback buffer will fill more than one page when printed, a range of pages to print can be selected. If any text is selected when you use the **Print** option, the default print range will be **Selection**, which will only print the currently selected text.

You can use the **Print Preview** option (see section 6.4 (Print Preview)) to help you to determine which pages to print and how the printout will look like.

Note: If you use a network printer, the area selected for printing will be sent unencrypted over the network to the printer. This is a security risk you should consider when printing confidential information.

The **Print** option is available only in the terminal window.

6.4 Print Preview

Select the **Print Preview** option to display the entire contents of the terminal scrollback buffer, split into pages in the same way as the scrollback buffer will appear when printed.

The following buttons can be used to preview the print result:

Print

The Print button opens the **Print** dialog, allowing you to specify the printer settings and print the result.

Next Page

 © 2002 SSH Communications Security Corp.

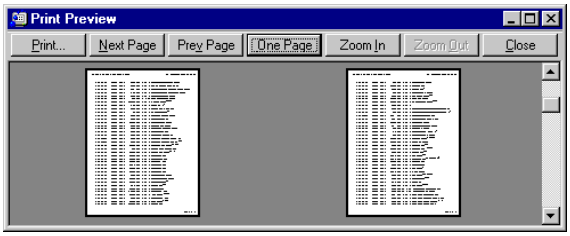

Figure 6.5: The Print Preview option show the scrollback buffer as it would appear when printed.

Click the Next Page button to preview the next page of output. The keyboard shortcut for Next Page is the `Page Down` key.

Prev Page

Click the Prev Page button to preview the previous page of output. The keyboard shortcut for Prev Page is the `Page Up` key.

One Page / Two Pages Toggle

Click the One Page / Two Pages Toggle button to display two pages of output side by side. When in two page print preview mode, the Two page button is replaced by One Page button, which allows you to return to the one page print preview mode. This button cannot be used when you have zoomed the page.

Zoom In

Click the Zoom In button to see a closeup of the currently displayed print preview page. You can use this button to zoom up to the natural size of the printout. You can zoom in also by clicking the left mouse button on the preview view.

Zoom Out

Click the Zoom Out button to return from a zoomed in view of the print preview page. You can zoom out until the whole page is displayed.

Close

Click the Close button to close the Print Preview dialog. The dialog can be closed also by pressing the `Esc` key.

The Print Preview option is available only in the terminal window.

6.5 Connect

Select the **Connect** option to connect to a remote host computer. A **Connect to Remote Host** dialog will open.

For more information on this dialog, see section 3.4.2 (Connect to Remote Host Dialog).

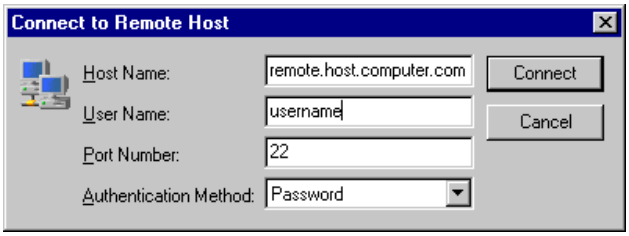

Figure 6.6: The Connect to Remote Host dialog.

6.6 Disconnect

Select the **Disconnect** option to quit the current connection. A **Confirm Disconnect** dialog is displayed, allowing you to confirm if you really want to disconnect. Select **Cancel** to keep the connection open, or **Yes** to end the connection. If you do not want to see the **Disconnect** confirmation dialog again, select the **Remember my answer** check box.

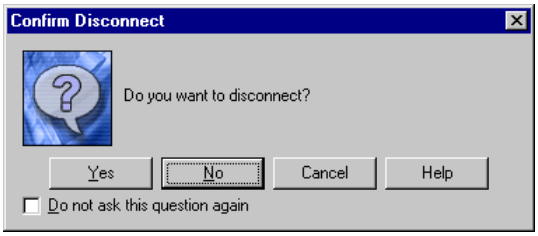

Figure 6.7: The Confirm Disconnect dialog gives you the last change option of changing your mind.

Note that one connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and a File Transfer window). Disconnecting affects all windows associated with a single connection.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but no other, separate connections.

6.7 Copy

Select the **Copy** option to create a temporary copy of the selected text or files.

If you are copying text (in the terminal window), the text is placed on the Windows clipboard and can be pasted in the terminal window or any Windows text window.

If you are copying files (in the **File Transfer** window), a **Download** dialog is displayed, but the selected files are not yet copied to any specific location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location.

 © 2002 SSH Communications Security Corp.

If you do a new copy operation when the previously copied text or files have not yet been copied anywhere, the previous selection is lost, as the new selection replaces the old one.

Note that the copy option is not available until you have selected some text (in the terminal window) or one or several files or folders (in the **File Transfer** window).

You can do a copy operation also by using the keyboard shortcut `Ctrl+Insert`. This shortcut is available in both **Terminal** and **File Transfer** windows.

6.8 Paste

Select the **Paste** option to add previously copied text or files or folders into a new location.

If you are pasting text (in the terminal window), the text that was copied earlier into the clipboard will be inserted in the cursor location. You can paste text that was copied from the terminal window or any other Windows text window.

If you are pasting files (in the File Transfer window), an **Upload** dialog is displayed when the files are pasted to the new location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location. The file names of the pasted files and folders do not change during the operation. Therefore it is not possible to paste files or folders several times into one location.

Note that the paste operation is not available until you have previously copied something in the clipboard.

You can do a paste operation also by using the keyboard shortcut `Shift+Insert` on the keyboard. This shortcut is available in both **Terminal** and **File Transfer** windows.

6.9 Paste Selection

Select the **Paste Selection** option to paste text into the terminal window without first copying anything to the clipboard. The **Paste Selection** operation copies whatever is currently selected in the terminal window to the present cursor position. If no text is selected, **Paste Selection** pastes the single character in the current cursor position.

This function is almost like having two different clipboards available at the same time. **Paste Selection** is especially useful for quick copying of text from the output of previous commands.

The **Paste Selection** toolbar button is available only in the terminal window.

6.10 Find

Select the **Find** option to locate text (or any other characters) from the scrollback buffer. Regular expressions can be used to select characters matching a specific pattern. The **Find** option is only available in the **Terminal** window.

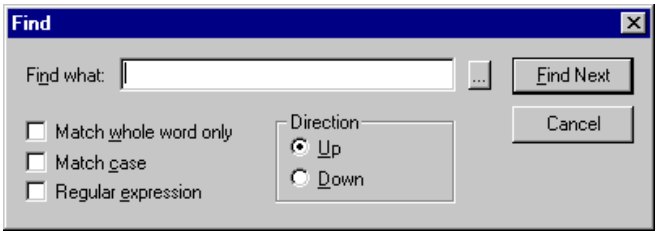

Figure 6.8: The Find dialog helps you to locate text from the scrollback buffer.

Find what

Type in the characters that you want to search for in the **Find what** field. If you want to use regular expressions to define the search term, select the **Regular expression** option, or select a ready defined regular expression by clicking the ellipsis button (. . .) on the right hand side of the **Find what** field.

...

Click the ellipsis button (...) to select from a ready list regular expressions. Using this option will turn on the Regular expression option.

The following regular expression types can be selected:

Any Character

Character in Range

Character not in Range

Beginning of Line

End of Line

Or

0 or More Matches

1 or More Matches

Optional Match

Match exactly n times

Match n or more times

Match at most n times

Match no less than n times and no more than m times

Match whole word only

Select the Match whole word only option to limit the search to match only whole words (i.e. so that ”wave” would not match ”waves”).

 © 2002 SSH Communications Security Corp.

Match case

Select the Match case option to specify that the search result should be case sensitive (i.e. so that ”Wave” would not match ”wave” or ”waVe”).

Regular expression

Select the Regular expression option to specify the search term using regular expressions. This option is automatically selected if you click the ellipsis button (...) on the right hand side of the Find what field.

Direction

Use the Direction option to specify whether the search should start upwards on downwards from the present position in the scrollback buffer.

The direction of the search is relative to the last match made in the current search. If there have been no previous matches, Up will search from the bottom of the buffer upwards, and Down will search downwards from the very beginning of the buffer.

Up

The Up option specifies that the search should start backwards from the present position.

Down

The Down option specifies that the search should start forward from the present position.

Find Next

Click the Find Next button to find the next match for the search term. Note that the direction where the search will continue is defined by the Direction option.

Cancel

Click the Cancel button to close the Find dialog.

6.11 New Terminal Window

Select the **New Terminal Window** option to open a new SSH Secure Shell for Workstations Windows client **Terminal** window. The new window is immediately connected to the same remote host computer as the current window, saving you the trouble of typing your password again.

Multiple windows to a single connection allow you to for example debug your code in one window, execute it in another, display reference information in a third one and read your mail in a fourth window.

The sequence number of each window is displayed on the window’s title bar, in front of the remote host computer’s name. For example, a second window associated with a connection to a host computer called remote would display as `2:remote`.

Note: To close any extra windows when you no longer need them, click on the X-shaped close button located on the window’s title bar on the upper right hand corner of the window. Do not click on the **Disconnect** button or select the **Disconnect** option from the **File** menu, as this would close the connection in all windows associated with this particular connection.

6.12 New File Transfer Window

Select the **New File Transfer Window** option to open a **File Transfer** window. To make file handling as easy as possible, you can open an unlimited number of **File Transfer** windows.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a third window associated with a connection to a host computer called remote would display as `3:remote`.

Note: To close any extra windows when you no longer need them, click on the X-shaped close button located on the window's title bar on the upper right hand corner of the window. Do not click on the **Disconnect** button or select the **Disconnect** option from the File menu, as this would close the connection in all windows associated with this particular connection.

6.13 Settings

Select the **Settings** option to bring up the **Settings** dialog. Settings can be used to control both the global settings and the profile settings for each particular remote host computer. For more information on the **Settings** dialog, see chapter 2 (Configuration).

6.14 Contents

Select the **Contents** option to display the contents of the SSH Secure Shell Windows client help. In the help window you can browse, search and print help information.

6.15 Get Help On

Select the **Get Help On** option to change the mouse pointer to a help pointer. You can use the help pointer to click on buttons, menu items or other details of the user interface to see context sensitive help on any particular item.

6.16 File Transfer Specific Toolbar Buttons

The following toolbar buttons are available only in the File Transfer window.

 © 2002 SSH Communications Security Corp.

Figure 6.9: The buttons that are available only in the File Transfer window are located between the Settings button and the Contents button.

6.16.1 Download Dialog

Select the **Download Dialog** option to open the **Download - Select Folder** dialog that allows you to select a folder on the local computer and transfer the currently selected file into it. The shortcut key for Download Dialog is `Ctrl+D`.

6.16.2 Upload Dialog

Select the **Upload Dialog** option to open the **Upload - Select Files** dialog that allows you to select a file and transfer it from the local computer into the remote host computer. The shortcut key for Upload Dialog is `Ctrl+U`.

6.16.3 Toggle Transfer View

Select the **Toggle Transfer View** option to hide or show the **Transfer View** pane.

6.16.4 Large Icons

Select the **Large Icons** option to display the file view as a Large Icons view. Each file and folder has a large icon associated with it, making for a clear and uncluttered display.

6.16.5 Small Icons

Select the **Small Icons** option to display the file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

6.16.6 List

Select the **List** option to display the file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

6.16.7 Details

Select the **Details** option to display the file view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, last modification date and attributes visible.

By clicking on the Name, Size, Type and Modified sort bars located on top of the File view, you can sort the files and folders based on their file name, file size, file type and the time they were last modified. Selecting the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file types are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the remote computer.

6.16.8 ASCII

Select the **ASCII** option to transfer files in ASCII mode.

6.16.9 Binary

Select the **Binary** option to transfer files in binary mode.

6.16.10 Auto Select

Select the **Auto Select** option to automatically change the transfer mode based on the file extension. Files using a file extension specified on the **ASCII Extensions** list on the **Mode** page of the **Settings** dialog will be transferred in ASCII mode. All other files will be transferred in binary mode. For more information, see section 2.4.19 (Mode).

6.16.11 Cancel Transfer

Select the **Cancel Transfer** option to stop ongoing file transfers.

6.17 Profiles Bar

The **Profiles** bar contains buttons that allow a fast way to connect to different servers.

Quick Connect

 © 2002 SSH Communications Security Corp.

Click the **Quick Connect** button on the profiles toolbar to open a new connection using the default settings. For more information, see section 3.1 (Quick Connect).

Profiles Button

Click the Profiles button on the profiles toolbar to open the Profiles menu. For more information on how to use profiles, see section 3.2 (Profiles).

6.18 File Bar

The **File** bar contains buttons that can be used to perform the most commonly used file management tasks. The file bar is dynamically created, so it cannot be customized like the other toolbars.

Note: It is possible to have the file bar trimmed down so that it shows less buttons and leaves more room for the favorite folders lists. The file bar with the wide folder view displays only the **Show/Hide Local Folders**, **Local Home** and **Up** buttons above the Local View, and the corresponding **Show/Hide Remote Folders**, **Remote Home** and **Up** buttons above the Remote View. See 2.4.17 (File Transfer) for more information.

6.18.1 Show/Hide Local Folders

Select the **Show/Hide Local Folders** option to toggle whether the folder view of the local directory is displayed. The folders are displayed on the edge of the **Local View** pane.

6.18.2 Local Home

Select the **Home** option to return to your home directory on the local computer. This is useful if you are exploring a complex directory tree and want to quickly return to where you came from.

6.18.3 Up

Select the **Up** option to move the view from the current folder to its parent folder.

For example: You have a directory called `home` and it has a subdirectory called `mail`. If you are currently viewing the `mail` folder and click the **Up** button, the focus moves to the `home` folder.

6.18.4 Refresh Local

Select the **Refresh Local** option to redraw the contents of **Local View**. This may be necessary if you have for example downloaded a file that does not immediately become visible in **Local View**.

6.18.5 New Local Folder

Select the **New Local Folder** option to create a new subdirectory in the current local directory. A new folder icon appears in **Local View** and you can type in the name of the new folder. (If you do not enter a name for the folder, it will not be created.)

6.18.6 Delete Local

Select local files or folders that you want to remove, and then select the **Delete Local** option to remove them. A **Confirm Delete** dialog will be displayed, asking you to confirm the removal.

6.18.7 Local Favorites

You can use the **Local Favorites** drop-down list box to open the contents of other local drives and directories in **Local View**. You can customize the contents of the **Local Favorites** list on the **Local Favorites** page of the **Settings** dialog (see section 2.4.20 (Local Favorites)).

6.18.8 Add

Select the **Add** option to add the current directory in the **Local Favorites** list.

6.18.9 Show/Hide Remote Folders

Select the **Show/Hide Remote Folders** option to toggle whether the folder view of the remote directory is displayed. The folders are displayed on the edge of the **Remote View** pane.

6.18.10 Remote Home

Select the **Remote Home** option to return to your home directory on the remote computer. This is useful if you are exploring a complex directory tree and want to quickly return to where you came from. The shortcut key for the **Remote Home** option is `Ctrl+H`.

6.18.11 Up

Select the **Up** option to move the view from the current folder to its parent folder.

For example: You have a directory called `home` and it has a subdirectory called `mail`. If you are currently viewing the `mail` folder and click the **Up** button, the focus moves to the `home` folder.

 © 2002 SSH Communications Security Corp.

6.18.12 Refresh Remote

Select the **Refresh Remote** option to redraw the contents of **Remove View**. This may be necessary if you have for example uploaded a file that does not immediately become visible in **Remote View**. The shortcut key for the **Refresh** option is `F5`.

6.18.13 New Remote Folder

Select the **New Remote Folder** option to create a new subdirectory in the current remote directory. A new folder icon appears in **Remote View** and you can type in the name of the new folder. (If you do not enter a name for the folder, it will not be created.) The shortcut key for the **New Remote Folder** option is `Ctrl+N`.

6.18.14 Delete Remote

Select remote files or folders that you want to remove, and then select the **Delete Remote** option to remove them. A **Confirm Delete** dialog will be displayed, asking you to confirm the removal.

6.18.15 Remote Favorites

You can use the **Remote Favorites** drop-down list box to open the contents of other remote drives and directories in **Remote View**. You can customize the contents of the **Remote Favorites** list on the **Remote Favorites** page of the **Settings** dialog (see section 2.3.9 (Remote Favorites)).

6.18.16 Add

Select the **Add** option to add the current directory in the **Remote Favorites** list.

© 2002 SSH Communications Security Corp.

Chapter 7

Menu Reference

Together with the toolbar, the menus allow quick access to different terminal and file transfer operations. The following menus are available: **File**, **Edit**, **View**, **Operation** (only in the **File Transfer** window), **Window** and **Help**.

7.1 Configuring Menus

The SSH Secure Shell menus can be configured as easily as the toolbars. You can freely select the position of the menus, and even move them into toolbars.

7.1.1 Moving Menus

You can move the SSH Secure Shell menus into new positions and arrange them so that they best serve your needs.

To move a menu, keep the `Alt` key on the keyboard pressed down and click a menu with your mouse. You will see a new mouse pointer appear. Keep the mouse button pressed down and move the menu around. When you release the mouse button, the menu will be move to a new position.

This way you can arrange the order of the menus, or even move menus into toolbars. Experiment to find the best configuration for you.

It also possible to move the individual menu options. This can be done using the **Commands** page of the **Customize** dialog (see section 2.5 (Customize)).

Note: If you move a menu to somewhere else than the menu bar or a toolbar (for example, in the terminal window text area), it is removed from the window. But don't worry - the changes become permanent only if you use the **Save Settings** option (see section 6.2 (Save Settings)).

 © 2002 SSH Communications Security Corp.

7.1.2 Permanent Menu Changes

If you want to make the new menu positions permanent, use the **Save Settings** option (from the toolbar or the **File** menu) to save your settings.

If you change your mind and want to return the menus to their original positions, select the **Reset Toolbars** option from the **View** menu. A confirmation dialog will open, asking if you really want to discard the changes you have made. If you select **Yes**, the menus will return to their original configuration. If have modified also your toolbars, this option will reset them, too.

7.2 File Menu

The **File** menu allows access to the settings file and connect/disconnect operations.

7.2.1 Save Settings

Select the **Save Settings** option to save any changes you have made to your current settings. The default settings file where the configuration will be saved is `default.ssh2`.

If you want to save your current settings in a new settings file, select **Add Profile** from under the **Profiles** option (see section 3.2 (Profiles)).

7.2.2 Save Layout

Select the **Save Layout** option to save both the current settings and the current window layout.

7.2.3 Quick Connect

Select the **Quick Connect** option from the **File** menu to open a new connection using the default settings. For more information, see section 3.1 (Quick Connect).

7.2.4 Profiles

Select the **Profiles** option from the **File** menu to open the **Profiles** menu. For more information on how to use profiles, see section 3.2 (Profiles).

7.2.5 Print

The **Print** option allows you output the contents of the current scrollback buffer to a printer. For more information on printing, see section 6.3 (Print).

The **Print** option is available only in the terminal window.

7.2.6 Print Preview

Selecting the **Print Preview** option will display the entire contents of the scrollback buffer split into pages in the same way it will be printed. For more information on previewing the printer output, see section 6.4 (Print Preview).

The **Print Preview** option is available only in the terminal window.

7.2.7 Page Setup

The **Page Setup** option allows you to specify how printed pages will look. For more information, see section 2.4.23 (Printing).

The **Page Setup** menu option is available only in the terminal window.

7.2.8 Log Session

Select the **Log Session** option to save an entire transcript of the current terminal session to a file.

When **Log Session** is selected, the **Save As** dialog opens, asking for a file name for the log file. This file will be created if it does not already exist, and it will contain a transcript of the connection. Selecting the **Log Session** menu item for a second time stops logging.

When logging is active, a checkmark appears next to the **Log Session** menu option.

The **Log Session** menu option is available only in the terminal window.

7.2.9 Connect

Select the **Connect** option to establish a new SSH connection to a remote host computer. A **Connect to Remote Host** dialog will appear, allowing you to specify the host name (or IP address), user name and password for the new connection.

An alternative way to establish a new connection is to press the `Enter` key on the keyboard when disconnected.

 © 2002 SSH Communications Security Corp.

Note: The **Connect** option is available only when you are not connected to any remote host computer. If you want to establish a completely new, separate SSH connection, select the **Quick Connect** option instead.

7.2.10 Disconnect

Select the **Disconnect** option to disconnect from the present remote host computer. A **Confirm Disconnect** dialog appears, allowing you to confirm if you really want to disconnect. Select **Cancel** to keep the connection open, or **Yes** to end the connection.

Note: One connection can have several windows open (such as a terminal window and a File Transfer window). Disconnecting affects all windows associated with a single connection.

However, if you have launched other, separate SSH Secure Shell clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but none of the separate connections.

7.2.11 Exit

Select the **Exit** option to quit the SSH Secure Shell client. A **Confirm Exit** dialog appears, allowing you to confirm if you really want to exit. Select **Cancel** to keep the Secure Shell client running, or **Yes** to exit.

Note: One connection can have several windows open (for example several File Transfer windows and several terminal windows). Exiting affects all windows associated with a single connection.

However, if you have started other, separate SSH Secure Shell clients, they are not affected by this exit operation. Exiting quits one connection and all of its associated windows, but none of the separate connections.

7.3 Edit Menu

The **Edit** menu allows you to copy and paste text in the terminal window and to make changes to your connection settings.

7.3.1 Copy

In the terminal window the **Copy** option can be used to copy selected text to the Windows clipboard.

In the File Transfer window the **Copy** option can be used to create a temporary copy of the selected file(s) in the File Transfer window. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location.

If you do a new copy operation when the previously copied files have not yet been copied anywhere, the previous selection is lost, as the new selection replaces the old one. Note that the copy operation is not available until you have selected one or several files or folders.

The keyboard shortcut for the copy option is `Ctrl+Insert`.

7.3.2 Paste

In the terminal window the **Paste** option can be used to attach previously copied text from Windows clipboard into the current cursor position.

In the File Transfer window **Paste** option can be used to add previously copied files or folders into a new location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location. You can do a paste operation also by pressing `Ctrl+V` on the keyboard.

The file names of the pasted files and folders do not change during the operation. Therefore it is not possible to paste files or folders several times into one location.

Note that the paste operation is not available until you have previously copied something in the clipboard. The keyboard shortcut for paste is `Shift+Insert`.

7.3.3 Paste Selection

The **Paste Selection** option is only available in the terminal window.

Select **Paste Selection** to paste text without first copying anything to the clipboard. The Paste Selection operation copies whatever is currently selected in the terminal window to the present cursor position. If no text is selected, Paste Selection pastes the single character in the current cursor position.

This function is almost like having two different clipboards available at the same time. Paste Selection is especially useful for quick copying of text from the output of previous commands.

7.3.4 Select All

Choose the **Select All** option to select all the text in the current terminal window and the scrollback buffer, or all the files and folders in the current directory in the File Transfer window.

Note that in the terminal window, the selection can span quite a few lines backwards from what is currently visible. If you want to select just what is currently displayed on screen, use the **Select Screen** menu option instead.

When used in the terminal window, this operation makes it fast and easy for example to save long command output strings or to create a temporary log of what is displayed on the screen.

 © 2002 SSH Communications Security Corp.

For file transfer, this enables you to operate on the whole contents of a directory at one time. This can be especially useful when downloading, copying or deleting files.

The keyboard shortcut for **Select All** is `Ctrl+A`.

7.3.5 Select Screen

The **Select Screen** option is available only in the terminal window.

Choose the **Select Screen** option to select all the text that is currently visible in the terminal window. Note that unlike the Select All option, Select Screen does not capture the scrollback buffer. This operation can be especially useful for screen captures and quick snapshots of the command output.

7.3.6 Select None

The **Select None** option is available only in the terminal window.

Choose the **Select None** option to cancel any previous selection. This operation immediately clears the selection in the terminal window.

7.3.7 Find

The **Find** option is available only in the terminal window.

Choosing the **Find** option allows you to search for text within the scrollback buffer. For more information on searching, see section 6.10 (Find).

7.3.8 Settings

Select the **Settings** option to bring up the **Settings** dialog. Settings can be used to control both the global settings and the profile settings for each particular remote host computer. For more information on the **Settings** dialog, see section 2 (Configuration).

7.4 Terminal Window View Menu Options

The **View** menu allows you to select the way the SSH Secure Shell client windows are displayed. The terminal window has different set of View menu options than the File Transfer window.

7.4.1 Toolbar

Select the **Toolbar** option to toggle the toolbar on and off. When the toolbar is visible, a checkmark appears next to the **Toolbar** option.

7.4.2 Status Bar

Select the **Status Bar** option to toggle the status bar on and off. When the status bar is visible, a checkmark appears next to the **Status Bar** option.

7.4.3 Profiles Bar

Select the **Profiles Bar** option to toggle the profiles bar on and off. When the toolbar is visible, a checkmark appears next to the **Profiles Bar** option.

7.4.4 Customize

Select the **Customize** option to modify the menu options, toolbars, menu settings and general settings. The **Customize** dialog opens. For more information on customizing the user interface, see section 2.5 (Customize).

7.4.5 Reset Toolbars

Select the **Reset Toolbars** option to reset the toolbar and menu positions to their original state. This is a good choice if you regret the changes you have made, or have misplaced some menu or toolbar option.

7.4.6 Reset Terminal

Select the **Reset Terminal** option to reset the terminal settings to the state they were in when connecting. This will clear the terminal window and the scrollback buffer and reset the keymap, character set and fonts.

7.5 File Transfer View Menu Options

The **View** menu allows you to select the way the SSH Secure Shell client windows are displayed. The File Transfer window has different set of View menu options than the terminal window.

 © 2002 SSH Communications Security Corp.

7.5.1 Toolbar

Select the **Toolbar** option to toggle the toolbar on and off. When the toolbar is visible, a checkmark appears next to the **Toolbar** option.

7.5.2 Profiles Bar

Select the **Profiles Bar** option to toggle the profiles bar on and off. When the toolbar is visible, a checkmark appears next to the **Profiles Bar** option.

7.5.3 File Bar

Select the **File Bar** option to toggle the file bar on and off. When the toolbar is visible, a checkmark appears next to the **File Bar** option.

7.5.4 Status Bar

Select the **Status Bar** option to toggle the status bar on and off. When the status bar is visible, a checkmark appears next to the **Status Bar** option.

7.5.5 Local View

Select the **Local View** option to toggle Local View on and off. When Local View is visible, a checkmark appears next to the **Local View** option.

7.5.6 Transfer View

Select the **Transfer View** option to toggle Transfer View on and off. When Transfer View is visible, a checkmark appears next to the **Transfer View** option.

7.5.7 Customize

Select the **Customize** option to modify the menu options, toolbars, menu settings and general settings. The **Customize** dialog opens. For more information on customizing the user interface, see section 2.5 (Customize).

7.5.8 Reset Toolbars

Select the **Reset Toolbars** option to reset the toolbar and menu positions to their original state. This is a good choice if you regret the changes you have made, or have misplaced some menu or toolbar option.

7.5.9 Large Icons

Select the **Large Icons** option to display the file view as a Large Icons view. Each file and folder has a large icon associated with it, resulting in a clear and uncluttered display.

If the **Large Icons** option is selected, a selection marker appears next to the menu option.

7.5.10 Small Icons

Select the **Small Icons** option to display the file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

If the **Small Icons** option is selected, a selection marker appears next to the menu option.

7.5.11 List

Select the **List** option to display the file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

If the **List** option is selected, a selection marker appears next to the menu option.

7.5.12 Details

Select the **Details** option to display the file view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, last modification date and attributes visible.

By clicking on the **Name**, **Size**, **Type**, **Modified** or **Attributes** sort bars located on top of the folder view, you can sort the files and folders based on their file name, file size, file type, the time they were last modified and their file attributes. Selecting the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file types are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the host computer.

 © 2002 SSH Communications Security Corp.

7.5.13 Arrange Icons

Select the **Arrange Icons** option to open a submenu where you can select in which order the files and folders are displayed in the file view. A selection marker appears next to the currently selected Arrange Icons option.

By Name: The files and folders are arranged alphabetically based on their file name.

By Type: The files and folders are arranged alphabetically based on their file type.

By Size: The files are arranged by their file size. Folders are arranged alphabetically.

By Date: The files and folders are arranged by the time they were last modified.

If you have selected the **Details** view, you can achieve the same effect by clicking on the Name, Size, Type and Modified sort bars located on top of the folder view. Selecting the same **Arrange Icons** option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

7.5.14 Show Root Directory

Select the **Show Root Directory** option to toggle if the root directory is displayed in the folder view. If the root directory is not displayed, you are not able to select or view any folders above your home directory in the directory tree hierarchy. By default the root directory is not displayed.

If the **Show Root Directory** option is selected, a selection marker appears next to the menu option.

7.5.15 Show Hidden Files

Select the **Show Hidden Files** option to toggle if the normally hidden files are displayed in the folder view.

By default, UNIX hosts do not display any files or directories that begin with the dot (.) character, such as .rhosts or .profile. Selecting the Show Hidden Files option corresponds to specifying the `-a` switch of the ls command.

If the **Show Hidden Files** option is selected, a selection marker appears next to the Show Hidden Files menu option.

7.5.16 Refresh

Select the **Refresh** option to redraw the File Transfer window. This may be necessary if you have for example uploaded a file that does not immediately become visible on the remote host computer.

The keyboard shortcut for **Refresh** is `F5`.

7.6 Operation Menu

The **Operation** menu is available only in the File Transfer window.

The **Operation** menu allows you to copy files to and from the remote host computer, and to navigate the remote directory structure.

7.6.1 Open

The **Open** option can be used to view a file on the remote host computer. First select a file from the File Transfer window and the select the **Open** option. The file will be downloaded and displayed.

7.6.2 Upload

Select the **Upload** option to upload a file - i.e. to copy it from your local computer to the remote host computer (server). The keyboard shortcut for **Upload** is `Ctrl+U`.

7.6.3 Download

Select the **Download** option to download a file - i.e. to copy it from the remote host computer to your local computer.

Note that you must first select the remote file(s) before selecting Download. If no files or folders are selected, the Download menu option is grayed out. The keyboard shortcut for Download is `Ctrl+D`.

7.6.4 Upload Dialog

Select the **Upload Dialog** option to open the **Upload - Select Files** dialog that allows you to select a file and transfer it from the local computer into the remote host computer. The shortcut key for Upload Dialog is `Ctrl+U`.

7.6.5 Download Dialog

Select the **Download Dialog** option to open the **Download - Select Folder** dialog that allows you to select a folder on the local computer and transfer the currently selected file into it. The shortcut key for Download Dialog is `Ctrl+D`.

 © 2002 SSH Communications Security Corp.

7.6.6 Cancel

Select the **Cancel** option to stop ongoing file transfers.

7.6.7 Up

Select the **Up** option to move the view from the current folder to its parent folder.

For example: You have a directory called `home` and it has a subdirectory called `mail`. If you are currently viewing the `mail` folder and click the **Up** button, the focus moves to the `home` folder. The keyboard shortcut for **Up** is the `Backspace` key. This has the same effect as choosing the Upload option from the Operation menu or the toolbar.

7.6.8 Home

Select the **Home** option to return to your home directory. This is useful if you are exploring a complex directory tree and want to quickly return to where you came from. The keyboard shortcut for **Home** is `Ctrl+H`.

7.6.9 Go To Folder

Select the **Go to Folder** option to enter a remote folder where you want to move directly. A **Go to Remote Folder** dialog appears, allowing you to type in the path to the desired directory in the remote host computer. The current directory path is displayed in the text field for your reference, eliminating the need to type in long directory paths from scratch. Type in the desired directory path and press `Enter`. The specified directory instantly appears. The keyboard shortcut for Go To Folder is `Ctrl+G`.

7.6.10 New Folder

Select the **New Folder** option to create a new folder on the remote host computer. A new folder appears on folder view along with a text field where you can type in the name for the new folder.

If you do not type a name for the new folder but just hit `Enter`, a new folder is not created. The keyboard shortcut for **New Folder** is `Ctrl+N`.

7.6.11 Delete

Select the **Delete** option to delete file(s) or folder(s) on the remote host computer. A **Confirm Delete** dialog appears, allowing you to confirm if you really want to delete the selected files or folders. Select **Cancel** to keep the selected items, or **Yes** to delete them. The keyboard shortcut for Delete is the Delete key.

7.6.12 Rename

First select a file from the File Transfer window and then the **Rename** option to give the file a new name. The keyboard shortcut for rename is F2.

You can also rename a file by clicking on the file with the right mouse button. A shortcut menu containing the **Rename** option will appear.

Note: The rename operation requires an SSH Secure Shell server version 2.2.0 or later. Earlier SSH Secure Shell server versions do not support the rename operation, and using this option will produce the *Error Renaming File* message. For more information, see section 9.2.10 (Error Renaming).

7.6.13 Properties

Select first a file from the File Transfer window and then the **Properties** option to view the file properties.

You can also view a file's properties by clicking on the file with the right mouse button. A shortcut menu containing the **Properties** option will appear. You can select multiple files and view their properties.

For more details about the Properties page, see section 5.7 (File Properties).

7.6.14 File Transfer Mode

Select the **File Transfer Mode** option to set in which transfer mode files will be transferred. A submenu opens, containing the following options:

ASCII

Select the **ASCII** option to transfer files in ASCII mode.

Binary

Select the **Binary** option to transfer files in binary mode.

Auto Select

Select the **Auto Select** option to automatically change the transfer mode based on the file extension. Files using a file extension specified on the ASCII Extensions list on the **Mode** page of the **Settings** dialog will be transferred in ASCII mode. All other files will be transferred in binary mode. For more information, see section 2.4.19 (Mode).

 © 2002 SSH Communications Security Corp.

7.7 Window Menu

The **Window** menu allows you to open and close different types of windows.

7.7.1 New Terminal

Select the **New Terminal** option to open a new SSH Secure Shell client terminal window. The new window is immediately connected to the same remote host computer as the current window, saving you the trouble of authenticating yourself again.

Multiple windows to a single connection allow you to for example debug your code in one window, execute it in another, display reference information in a third one and read your mail in a fourth window.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a second window associated with a connection to a host computer called 'remote' would display as `2:remote`.

To close any extra windows when you no longer need them, click on the X-shaped close window button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

7.7.2 New File Transfer

Select the **New File Transfer** option to open a new File Transfer window. To make file managing as easy as possible, you can open an unlimited number of File Transfer windows.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a third window associated with a connection to a host computer called 'remote' would display as `3:remote`.

To close any extra windows when you no longer need them, click on the X-shaped close window button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

7.7.3 New Terminal in Current Directory

Select the **New Terminal in Current Directory** option to open a new terminal window in the current remote directory.

7.7.4 New File Transfer in Current Directory

Select the **New File Transfer in Current Directory** option to open a new File Transfer window in the current remote directory.

7.7.5 New Windows Explorer

The **New Windows Explorer** menu option is available only in the File Transfer window.

Select the **New Windows Explorer** option to open a new *Windows Explorer* window. The Windows Explorer is the familiar Windows utility that can be used to manage the files and folders on your local computer. You can have multiple Explorer windows open at the same time to make file management easier.

7.7.6 Close

Select the **Close** option to close the current window. Other windows are unaffected, even if they are associated with the same connection.

7.7.7 Close All Others

Select the **Close all Others** option to close all the other SSH Secure Shell client windows associated with the active connection.

A single connection can have several windows open (such as an SSH Secure Shell terminal window and a File Transfer window). The **Close All Others** operation affects all the other windows associated with a particular connection.

However, if you have started other, separate SSH Secure Shell clients, they are not affected by this operation. **Close All Others** only affects one connection and all of its associated windows, but no other, separate connections.

7.8 Help Menu

The **Help** menu allows you to access the help and copyright information.

7.8.1 Contents

Select the **Contents** option from the **Help** menu to view the help as Web pages. A browser will open and the HTML based help files will be loaded locally, from your own computer. The contents page will appear. Click

 © 2002 SSH Communications Security Corp.

on a chapter you want to explore, or click the Index link to see an alphabetical listing of keywords.

If you want to check the Web help instead of the locally installed help files, see the SSH Secure Shell for Workstations Windows client Web help: `http://www.ssh.com/products/ssh/winhelp/`.

7.8.2 Get Help On

Select the **Get Help On** option to change the mouse pointer to a help pointer. You can use the help pointer to click on buttons, menu items or other details of the user interface to see context sensitive help on any particular item.

7.8.3 SSH on the Web

Select the **SSH on the Web** option to open a submenu containing Web links to SSH Secure Shell Web pages.

Online Help

Select the **Online Help** option to load the Web version of the SSH Secure Shell for Workstations Windows client help (`http://www.ssh.com/products/ssh/winhelp/`). This is useful if you want to see the most up-to-date version of the help.

Frequently Asked Questions

Select the **Frequently Asked Questions** option to load the online version of the SSH Secure Shell for Workstations Windows client FAQ (`http://www.ssh.com/faq/`).

Home Page

Select the **Home Page** option to open the SSH Communications Security home page (`http://www.ssh.com`).

7.8.4 Troubleshooting

Select the **Troubleshooting** option to display the **Troubleshooting** dialog. If you encounter problems when using the SSH Secure Shell client, you can send a bug report by using the support web form at `http://www.ssh.com/support`. To make the support team's work easier, you should describe your system and the problem situation as carefully as possible. The Troubleshooting dialog helps you to achieve this.

Click the **Copy to Clipboard** button to copy the troubleshooting report on the Windows clipboard. You can then paste (`Ctrl+V`) the report into the support web form. But please describe your problem also in your own words - the Troubleshooting dialog cannot do that for you!

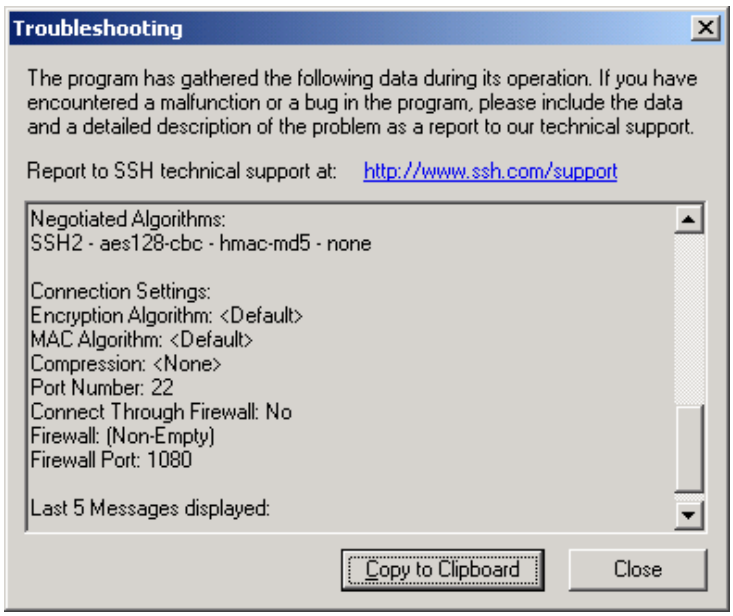
Troubleshooting
The program has gathered the following data during its operation. If you have encountered a malfunction or a bug in the program, please include the data and a detailed description of the problem as a report to our technical support.
Report to SSH technical support at: http://www.ssh.com/support
Negotiated Algorithms:
SSH2 - aes128-cbc - hmac-md5 - none
Connection Settings:
Encryption Algorithm: <Default>
MAC Algorithm: <Default>
Compression: <None>
Port Number: 22
Connect Through Firewall: No
Firewall: (Non-Empty)
Firewall Port: 1080
Last 5 Messages displayed:
Copy to Clipboard
Close

Figure 7.1: The Troubleshooting dialog.

7.8.5 Debugging

Select the **Debugging** option to gather debugging information useful for tracking possible errors. The Debugging dialog opens.

Enable Debugging

Select the **Enable Debugging** check box to log debugging information. Enabling this option slows down the client, so it should be only done to track error situations, for example when requested by SSH technical support.

Debug

The **Debug** options define how much debugging information will be collected and where the data will be saved.

Level

 © 2002 SSH Communications Security Corp.

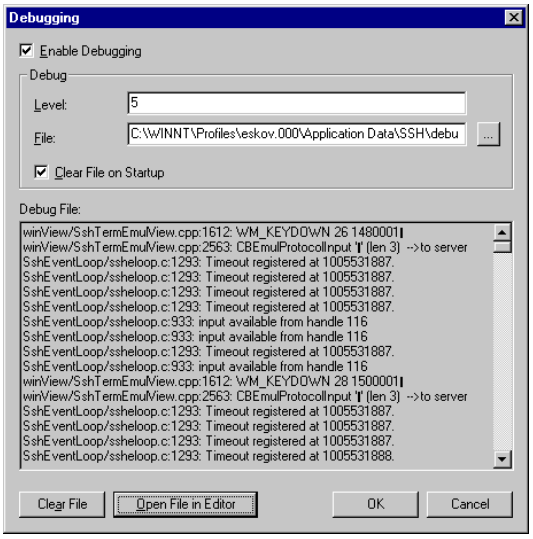

Figure 7.2: The Debugging dialog

Type in a number to indicate the debug level. Higher numbers will produce more debugging data. A typical value for debug level is 3 or 4. Debug levels approaching 10 will produce large amounts of debugging data and make the software very slow.

Alternatively you can specify different debug levels for different operations. For example the debug value `4, sshevent loop=7` would define the general debug level as 4, but for `sshevent loop` activity the debug level would be 7.

File

Select the file where debug data will be saved. Either type in the path and filename, or click the button on the righthand side of the text field to open a **Save As** dialog, allowing you to locate the save file.

Clear File on Startup

Select the **Clear File on Startup** check box to delete the debug data every time SSH Secure Shell is launched.

Note: If this option is not checked, the log file will keep continuosly growing and must be manually manually cleared.

Debug File

The **Debug File** displays a scrollable view of the currently gathered debug data.

Clear File

Click the **Clear File** button to empty the current debug data file.

Open File in Editor

Click the **Open File in Editor** button to open the current debug data file in a text editor, allowing you to view, edit, save or print the data.

OK

Click the **OK** button to accept the current settings and close the Debugging dialog.

Cancel

Click the **Cancel** button to discard the changes and close the Debugging dialog.

7.8.6 Import License File

With the **Import License File** option you can register your copy of the SSH Secure Shell for Workstations Windows client.

After you have applied for a license file from the SSH e-commerce web site (`http://commerce.ssh.com`) and received a license file (which is called `license.dat` by default), select the **Import License File** option from the **Help** menu. You will be presented with a dialog requesting a file name. Locate the `license.dat` file and click the **OK** button. You should see a dialog telling that the license file was successfully imported and copied to the installation directory. Click the **OK** button to continue. Your copy of the SSH Secure Shell for Workstations Windows client is now registered.

7.8.7 About Secure Shell

Select the **About Secure Shell** option to view the copyright information on SSH Communications Security's SSH Secure Shell for Workstations Windows client. Also version and license information is displayed. Click the **OK** button to close the dialog.

 © 2002 SSH Communications Security Corp.

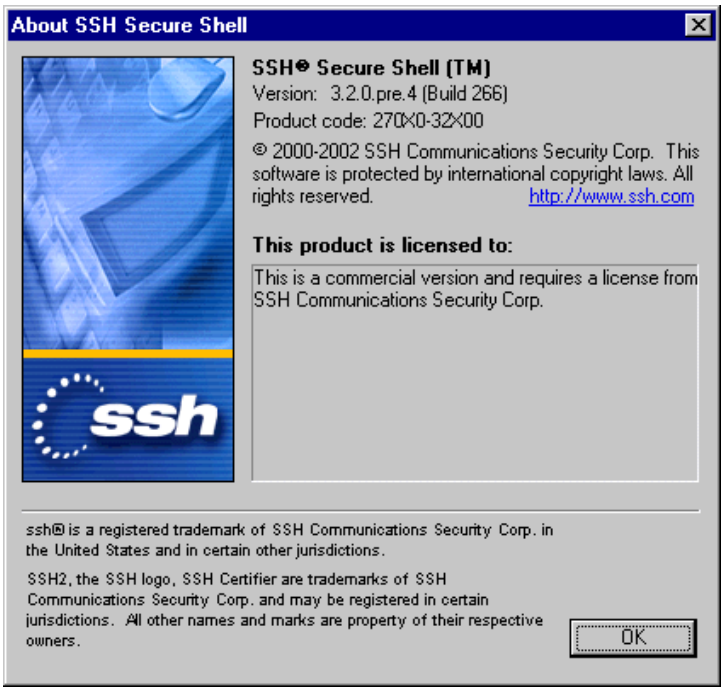
About SSH Secure Shell
SSH® Secure Shell (TM)
Version: 3.2.0.pre.4 (Build 266)
Product code: 270X0-32X00
© 2000-2002 SSH Communications Security Corp. This software is protected by international copyright laws. All rights reserved.
http://www.ssh.com
This product is licensed to:
This is a commercial version and requires a license from SSH Communications Security Corp.
ssh
ssh® is a registered trademark of SSH Communications Security Corp. in the United States and in certain other jurisdictions.
SSH2, the SSH logo, SSH Certifier are trademarks of SSH Communications Security Corp. and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.
OK

Figure 7.3: The About dialog displays copyright, licensing and version information.

Chapter 8

Advanced Information

SSH is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- Transport layer protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.
- User authentication protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol.
- Connection protocol [SSH-CONN] multiplexes several logical channels into the encrypted tunnel. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding (”tunneling”) arbitrary TCP/IP ports and X11 connections.

8.1 SSH2 Functionality

The SSH Secure Shell for Workstations Windows client connects and logs into the specified remote host computer. Upon login, the user must prove his identity to the remote host computer by using some authentication method.

 © 2002 SSH Communications Security Corp.

Public-key authentication is based on the use of digital signatures. Each user creates a public / private key pair for authentication purposes. The server knows the user's public key, but only the user has her private key.

When the user tries to authenticate herself, the server sends a challenge to the user. User is authenticated by signing the challenge using the private key.

Private / public key pairs can be created with a built-in key generation wizard. (See section 3.3.1 (Key Generation Wizard).)

Other authentication methods can be used as well. If other methods fail, the SSH Secure Shell for Workstations Windows client prompts for a password. Since all communications is encrypted, the password will not be available for eavesdroppers.

When the user's identity has been accepted by the server, the server either executes the given command, or logs into the remote host computer and gives the user a normal shell on the remote computer. All communication with the remote command or shell will be automatically encrypted. The session can be transparent and can be used to reliably transfer binary data.

The session terminates when the command or shell on the remote machine exits and all X11 and TCP/IP connections have been closed. The exit status of the remote program is returned as the exit status of `ssh2`.

If the user is using X11, the connection to the X11 display is automatically forwarded to the remote side in such a way that any X11 programs started from the shell (or command) will go through the encrypted channel, and the connection to the real X server will be made from the local machine.

SSH2 will also automatically set up Xauthority data on the server machine. For this purpose, it will generate a random authorization cookie, store it in Xauthority on the server, and verify that any forwarded connections carry this cookie and replace it by the real cookie when the connection is opened. The real authentication cookie is never sent to the server machine (and no cookies are sent in the plain).

If the user is using an authentication agent, the connection to the agent is automatically forwarded to the remote side unless disabled.

Forwarding of arbitrary TCP/IP connections over the secure channel can be specified. TCP/IP forwarding can be used for secure connections to electronic wallets or going through firewalls.

SSH2 automatically maintains and checks a database containing public keys of hosts. When logging on to a host for the first time, the host's public key is stored to a file in the user's personal directory. If a host's identification changes, SSH2 issues a warning and disables password authentication to prevent for example a malicious Trojan horse program from getting the user's password. Another purpose of this mechanism is to prevent man-in-the-middle attacks that could otherwise be used to circumvent the encryption.

SSH2 also has built-in support for SOCKS version 4 for traversing firewalls.

8.1.1 Host Keys

Each server host must have a host key. Hosts may have multiple host keys using multiple different algorithms. Multiple hosts may share the same host key. Every host must have at least one key using each required public key algorithm.

The server host key is used during key exchange to verify that the client is really communicating with the correct server. For this to be possible, the client must have prior knowledge of the server's public host key.

Two different trust models can be used:

- The client has a local database that associates each host name (as typed by the user) with the corresponding public host key. This method requires no centrally administered infrastructure, and no third-party coordination. The downside is that the database of name-key associations may become burdensome to maintain.
- The host name - key association is certified by a trusted certification authority. The client knows only the CA root key, and can verify the validity of all host keys certified by accepted CAs.

  The second alternative eases the maintenance problem, since ideally only a single CA key needs to be securely stored on the client. On the other hand, each host key must be appropriately certified by a central authority before authorization is possible. Also, a lot of trust is placed on the central infrastructure.

8.1.2 Security Properties

The primary goal of the SSH protocols is improved security on the Internet.

- All encryption, integrity, and public key algorithms used are well-known, well-established algorithms.
- All algorithms are used with cryptographically sound key sizes that are believed to provide protection against even the strongest cryptanalytic attacks for decades.
- All algorithms are negotiated, and in case some algorithm is broken, it is easy to switch to some other algorithm without modifying the base protocol.

8.2 Public-Key Infrastructure (PKI)

A system that uses digital certificates for authentication and thus helps establish secure communications is called a public-key infrastructure (PKI). A PKI consists of end entities, certification authorities (trusted parties who sign and issue certificates), and registration authorities (parties who handle the identification of end entities).

(Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.)

 © 2002 SSH Communications Security Corp.

A PKI provides a means for reliable authentication of parties in an online environment by using asymmetric encryption. In addition to authentication, the PKI also enables secure digital communications and transactions.

In asymmetric encryption, every entity (communicating party) has a key pair that consists of a public key and a private key. Private keys are secret and are known only to their owners. Private keys are used for signing and decrypting messages.

Public keys are, as the name implies, public and can be published on, for example, a web server. Public keys are used for validating signatures and encrypting messages. Before public-key operations can be made, the public key has to be received securely so that no one can substitute the genuine key with a tampered one. Certificates can be used for distributing public keys of end entities.

Certificates are digital documents that are used for secure authentication of communicating parties. Certificates are also used for sending the public keys of the entities to other entities. A certificate binds identity information about an entity to the entity's public key for a certain validity period. Certificates can be thought of as analogous to passports that guarantee the identity of their bearers.

To enable wide usage of certificates and interoperable implementations from multiple vendors, certificates have to be based on standards. The most advanced and widespread certificate specifications at the moment are defined by the PKIX Working Group of the IETF (Internet Engineering Task Force).

8.2.1 CA

The trusted parties that sign, issue and manage certificates are called certification authorities (CA). A CA is the instance that vouches for the identity and trustworthiness of the end entity it grants the certificates to. Certification authorities can be thought of as being analogous to governments issuing passports for their citizens.

CA can be a third party trusted by everyone in the PKI, or it can belong to the same organization as the end entities. CAs can also certify other CAs (to issue certificates) by signing so-called CA certificates. This leads to a tree-like structure of CA hierarchies. The top CA in the "tree" is called a root CA. A new root CA is established in two steps:

1. Generation of a CA key pair and a CA certificate.

2. Exporting the CA public key "out-of-band" to all end entities in the PKI.

The public keys of CAs are usually built into specific client applications. CA keys are then distributed when the client applications are installed to the end users' devices (workstations, laptops, PDAs). Before end entities can communicate securely, also their public keys need to be certified by enrolling the end entities into the PKI and having their certificates issued by the CA.

8.2.2 Certificate Enrollment

Certificate enrollment is an action in which a CA certifies a public key. A certification authority can delegate authentication of the end entities as well as certain other administrational tasks to so-called registration authorities (RA). Using local RAs a large geographically or operationally distributed PKI can work in a scalable way, even when the actual certificate issuing is centralized.

The actual enrollment process consists of the following steps:

1. Generation of a key pair
2. End entity requesting certification for the public key
3. CA or RA verifying the identity of the end entity
4. CA generating a certificate for the end entity and making it available (if the request is approved).

End entities can use standard request formats to request certificates from a CA. The CA uses the underlying policy to decide whether to approve the request or not. The policy decision and the approval/denial can be automatic, or it may be required that the operator of the CA has to approve certificate requests manually. If identification of the end entity is needed, the RA may perform this function. If the request is approved, a signed certificate will be issued and delivered to a public directory. Finally, when the issued certificates are available in the directories, all entities in the PKI can verify each other's certificates with the CA's public key.

8.2.3 Certificate Revocation

If a private key of an end entity is compromised or the right to authenticate with a certificate is lost during the certificate's validity period, the certificate has to be revoked, and all PKI users have to be informed about this. Certificate revocation lists (CRL) can be used for this purpose.

A CRL is a time-stamped list identifying the revoked certificates and is signed by a CA. The presence of the signature allows CRLs to be distributed via un-trusted channels in public directories, just like the certificates. Each CA issues CRLs on a regular basis, the issuance period being defined in the CA's security policy. Certificate validation has to include the retrieval of the latest CRL to check the status of the certificate. X.509 v2 CRL is a standard PKIX CRL format.

As the certificate revocation lists are updated on a periodic basis, they don't provide real-time status information for the PKI. If more strict security needs to be followed, online status data has to be provided for relying end entities. In Online Certificate Status Protocol (OCSP) OCSP responders respond to end entities' status requests with signed responses about the revocation status of a certificate. This kind of function is required for example in a PKI where high-value business transactions are digitally signed.

 © 2002 SSH Communications Security Corp.

8.2.4 Directory Services

Certificates and CRLs have to be distributed to directories in order to be available to PKI users. Information about how CRLs are to be obtained can be indicated in an extension field (distribution point) of an X.509 v3 certificate.

The Lightweight Directory Access Protocol (LDAP) has become a de facto standard procedure for CRL and certificate distribution. This enables interoperability with third party directory servers based on the LDAP standard. OCSP can be seen as an replacement for LDAP since with it revocation lists are not needed. However, encryption certificates still need to be fetched from somewhere, such as an LDAP directory.

8.3 Using Certificate Authentication

In order to use certificate authentication you need to issue certificates for users and hosts using a certification authority (CA) software such as SSH Certifier(TM).

The first requirement for using certificates is to import the certificates of the CAs that you trust. Trusting a CA means that to the best of your knowledge the private key of the CA has not been compromised. The CA certificates will be the connecting links between entities that have been issued a certificate.

Requesting a CA to issue a certificate is called *certificate enrollment*. SSH Secure Shell supports the CMPv2 enrollment protocol. If CMPv2 is not available in the CA software, the enrollment can be done in another application and the resulting certificates can be imported to SSH Secure Shell using the PKCS #12 format.

PKCS #12 format files can contain one or more user or CA certificates and private keys. SSH Secure Shell determines the contents of the file and writes the entries to the corresponding directories for subsequent use. Standard PKCS #12 files generated using applications such as Netscape Navigator and Microsoft Internet Explorer are supported.

Other supported formats for importing user and CA certificates are PKCS #7, BER and X.509 binary. If a user certificate is imported the corresponding private key must be made available to SSH Secure Shell. For this purpose, PKCS #12 is recommended.

In the certification request you can suggest a Common Name (e.g. *John Smith*), Organization Unit (like *Marketing*), Organization (*SSH Communications Security Corp.*), Country (*US*) and Email Address (*john.smith@ssh.com*).

The CA can change these fields before issuing the certificate. The certificate validity period and other parameters are determined by the configuration of the CA software. Please note that certificate enrollment requiring manual acceptance in the CA software is not supported. You may be able to compensate this by using PKCS #12 file importing.

8.3.1 PKCS #11

PKCS #11 is a runtime interface to hardware tokens and software keys. To be able to use a hardware token, such as a smart card or a USB token, a third party driver is required. The driver is usually a single DLL (Dynamic Link Library) file residing in the Windows system directory. You need to install the software included with the hardware token before configuring SSH Secure Shell.

8.4 Keyboard-Interactive Authentication

8.4.1 Overview

What Is Keyboard-Interactive?

Keyboard-interactive is a relatively new authentication method, designed in the Secure Shell Working Group. The Working Group's abstract contains the following introduction to the subject:

This document describes a general-purpose authentication method for the SSH protocol, suitable for interactive authentications where the authentication data should be entered via a keyboard. The major goal of this method is to allow the SSH client to support a whole class of authentication mechanism(s) without knowing the specifics of the actual authentication mechanism(s)

What Can Be Done with It?

Basically, any currently supported authentication method that requires only the user's input, can be performed with keyboard-interactive.

Currently, the following methods are supported:

- password
- SecurID
- PAM (but see Section 8.4.1 (What Cannot Be Done With It?)).

New authentication methods that can be implemented with this method include, but are not limited to, the following:

- S/KEY (and other One-Time-Pads)
- hardware tokens printing a number or a string in response for a challenge sent by the server. (Like SecurID, but there are others like that.)
- legacy authentication methods.

 © 2002 SSH Communications Security Corp.

What Cannot Be Done with It?

If passing of some binary information is required (as in public-key authentication), keyboard-interactive cannot be used.

PAM has support for binary messages and client-side agents, and those cannot be supported with keyboard-interactive. However, currently there are no implementations that take advantage of the binary messages in PAM, and the specification may not be cast in stone yet.

Chapter 9

Troubleshooting

If you should encounter an error message when using the SSH Secure Shell for Workstations Windows client, please read the error message carefully and follow the suggested course of action. Some possible error messages and their suggested corrective actions are described below.

9.1 Error Dialogs At Startup

If you get an error dialog when you try to run SSH Secure Shell, you may need to update the common controls library, `comctl32.dll`. The older library version is included in at least some Windows 95 installations. To obtain the update, go to the Microsoft web site `http://www.microsoft.com/msdownload/ieplatform/ie/comctrl x86.asp` and download the latest version.

9.1.1 Evaluation Period Ending

This message indicates that the evaluation period for this copy of SSH Secure Shell client will soon end. You are allowed to use the client for free for the duration of the evaluation period, and after that you should obtain a license in order to continue using the software.

For more information on the license agreement, read the file license.txt located in the directory where SSH Secure Shell for Workstations Windows client was installed.

Now is a good time to register the software to ensure that your network connections will always be secure. The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

 © 2002 SSH Communications Security Corp.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell Windows Client software, you can download the whole package with the license already installed.

Thank you for evaluating the SSH Secure Shell Windows Client!

9.1.2 Expiration

This error indicates that the evaluation period for this copy of the SSH Secure Shell client has ended. The client software cannot be used until you obtain a valid license.

For more information on the license agreement, read the file license.txt located in the same directory as the SSH Secure Shell Windows Client.

The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell Windows Client software, you can download the whole package with the license already installed.

Thank you for evaluating the SSH Secure Shell for Workstations!

9.1.3 Failed To Read Keymap File

This error message indicates that for some reason the SSH Secure Shell for Workstations Windows client is unable to read the KEYMAP.MAP file. When the Secure Shell client is started for the first time, it checks for the existence of the keymap file, and if the client does not find it, it copies it to the current user's personal directory.

For easy access to your personal data files, open the Profile Settings page of the Settings dialog and click the Browse button.

Check that the KEYMAP.MAP file is in the correct folder and that its Read-only attribute is not set.

9.1.4 File Open Error

This error indicates that a configuration file (such as KEYMAP.MAP or default.ssh2) could not be properly opened. The file may be damaged, or the file may define an unknown configuration value.

This error may indicate that you are using a configuration file that was created using an earlier version of the SSH Secure Shell client. You can remedy this by saving your configuration file again (select the Save option from the File menu).

9.1.5 Keymap Error

This error indicates that the SSH Secure Shell client has not been able to read a keymap file (`KEYMAP.MAP`, `KEYMAP22.MAP` or `OUTPUT.MAP`) that defines how the keyboard input/output is processed. The keymap file is either missing, corrupted or renamed with an unrecognizable file name.

Close the SSH Secure Shell client and check the keymap file.

9.1.6 Your License Has Expired

This error indicates that the license for this copy of the SSH Secure Shell for Workstations Windows client has expired. The client software cannot be used until you obtain a new license.

For more information on the license agreement, read the file license.txt located in the same directory as the SSH Secure Shell Windows Client.

The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell for Workstations software, you can download the whole package with the license already installed.

Thank you for using the SSH Secure Shell for Workstations Windows client!

 © 2002 SSH Communications Security Corp.

9.2 Error Dialogs During Operation

The following error dialogs may occur when operating SSH Secure Shell.

9.2.1 Authentication Failure

This error message indicates that the authentication process between your local computer and the remote host computer has for some reason failed.

The most common cause for failed authentication is an incorrect password, likely caused by a typing mistake.

Also the user name may be incorrect. Check that you have typed it correctly.

One possible reason for authentication failure is that the remote host computer may have been configured to require several authentication methods to be used. For example both password and public key authentication could be used for increased security. Even if you entered your password correctly, some other required authentication method could have failed. A relatively common situation is one where the remote host computer is expecting public-key authentication and you have not sent your public key to the host. You can do this by following the instructions in section 3.5 (Uploading Your Public Key).

It may also be possible that your account on the remote host computer has been disabled or that the remote host computer is having temporary problems causing errors with the login procedure.

Try to connect again and carefully type in your user name and password. If after a couple of retries you are sure that you have entered both of them correctly, contact the system administrator of the remote host computer.

9.2.2 Confirm Disconnect

This dialog is displayed when you are disconnecting an active connection. You can either confirm the disconnect operation or cancel it.

Yes

Click the Yes button to close the currently active connection.

Cancel

Click the Cancel button to change your mind and abort the disconnect operation. This has the same effect as selecting No. (This option is included to make the selection more intuitive for users who have clicked the Disconnect button in error.)

Help

Click the Help button to view the help.

Note that one connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and a File Transfer window). Disconnecting affects all windows associated with a single connection. All tunnels associated with the disconnected connection will be terminated as well.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but no other, separate connections. You can differentiate between different windows associated with a single connection by the window's sequence number, displayed on the title bar.

You can differentiate between different windows associated with a single connection by the window's sequence number, displayed on the title bar (see section 4.1 (Terminal Window Title Bar)).

9.2.3 Confirm File Overwrite

The Confirm File Overwrite dialog indicates that a file you are transfering already exists in the target system. You can choose if you want to replace the old file with the transferred file.

You have the following options:

Yes

Click the Yes button to replace the old file.

Yes to All

Click the Yes to All button to replace this file and also all the other files that already exist in the target system.

Cancel

Click the Cancel button to abort the file transfer operation.

9.2.4 Connection Failure

This error indicates that the SSH Secure Shell client cannot establish a connection to the remote host computer. There are several reasons that might cause this situation.

It may be that you have simply made a typing mistake, and there is an error in the name of the remote host computer. In this case you should also receive an error stating that the host is unknown.

Check that you have defined the correct port number for the connection. The port can be changed on the Connection page of the Settings dialog.

There may be problems with the configuration or physical setup of the network connection. Verify that other network connections are functioning.

 © 2002 SSH Communications Security Corp.

This problem may also arise if your local system is protected by a firewall and the firewall has not been properly configured. If you suspect that this is the case, ask your local system administrator to reconfigure the firewall.

There may also be a temporary problem with the remote host computer. If this is the case, you should wait for a while and try to connect again later. Contact the administrator of the remote host computer for additional information.

9.2.5 Disconnected; Authentication Error

The error message "Disconnected; Authentication Error (No further authentication methods available.)" indicates that any of the methods that have been used to authenticate you to the server have not been successful.

A relatively common situation is one where the remote host computer is expecting public-key authentication to be used and you have not sent your public key to the host. You can do this by following the instructions in section 3.5 (Uploading Your Public Key).

This error is also produced if the system's name server is not doing reverse lookups correctly. Ask your system administrator to configure the name server so that it does reverse lookups properly.

If this is not possible, the system administrator has to edit the file `/etc/ssh2/sshd2_config` on the Secure Shell server and change the `RequireReverseMapping` setting to `no`.

This is a common problem for modem connections. Typical modem connections use dynamic IP addresses. This means that the IP address changes from one connection to another, and these dynamic IP addresses have no permanent name server entries in the Domain Name System (DNS). If this is the case, you will have to ask your service provider to edit the sshd2_config file on the SSH server.

9.2.6 Disconnection

This error indicates that the connection to the remote host computer has been lost.

There may be problems with the configuration or the physical setup of either your or the remote host computer's network connection.

It may also be that the remote host computer has been rebooted, which has disconnected your computer from the host.

Usually problems of this kind are temporary, and you can try again after waiting for a while. If this does not help, check your local network, and if necessary, contact also the system administrator of the remote host computer.

9.2.7 Enter Passcode

When using SecurID for authentication, you have to enter the passcode in order to authenticate the connection. In some situations you may not be able to do this immediately, but will have to wait for the token to change.

9.2.8 Enter Passphrase For Private Key

This message indicates that the remote host computer is willing to accept your public key to authenticate you in the future.

Type in the passphrase associated with this key. (You defined the passphrase when you created the public key - see section 3.3.5 (Key Generation - Enter Passphrase) for more information.)

If you just press the Enter key, public authentication will not be used, and the system will ask you to type in your password instead.

9.2.9 Enter PIN

When using certificate authentication, the Enter PIN dialog will display information on the provider used. You will have to enter the personal identification number (PIN) associated with the token.

9.2.10 Error Renaming

This error message indicates that a file or folder on the remote host computer could not be renamed. Usually this means that the SSH server software is too old to support renaming.

The rename operation requires an SSH Secure Shell server version 2.2.0 (or later). Earlier SSH Secure Shell server versions do not support the rename operation. Renaming remote files or folders is not possible until the system administrator of the remote host computer updates the SSH server software.

9.2.11 Failed To Create An Incoming Tunnel

This error indicates that the system has not been able to create the requested tunnel.

The most common reason for this failure is that a tunnel with the same name already exists. The similarly named tunnel may have been created by another SSH Secure Shell client connected to the same server.

If the system has several of Secure Shell users, they may already have reserved several available ports. In this case just try again to find a free port.

Another possible reason is that you have no permission to open the requested port. The system administrator may have set a policy that restricts opening of communications ports - this is common practice especially

 © 2002 SSH Communications Security Corp.

with incoming ports. Check the local policy from the system administrator. Please note that only the system administrator (root) can open port numbers under 1024.

Please note that both incoming and outgoing tunnels produce their own error messages. If both fail, the client will display two separate error messages.

9.2.12 Host Identification

When you connect to a remote host computer for the first time, the host sends your local computer its public key in order to identify itself. To help you to verify the host's identity, the Host Identification dialog displays a fingerprint of the host's public key. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable series of five lowercase letters separated by dashes. If you have reason to suspect that the public key you have received may be forged, you can for example phone the system administrator of the remote host computer and check if the fingerprint is correct.

You can save the host key on your local computer by clicking the Yes button. This is the recommended action. If you save the host key, you won't have to answer this dialog again when connecting to the same host from the same computer.

If you do not want to save the host key, click the No button. You can connect normally, but the next time you connect to the same host, the remote host will send you its public key and you will again be asked, if you want to save the key on your local computer.

You can also cancel the connection attempt by clicking the Cancel button. This results in an authentication failure, and the connection will be canceled. The host key is not saved and your local computer will not be no connected to the remote host computer.

9.2.13 Host Identification Failed

This error signifies that the identification method used by the remote host computer does not match what was expected by the SSH Secure Shell client.

A change in the host identification may be caused by one of the following reasons:

- The administrator of the remote host computer has changed the identification method.
- The administrator of the remote host computer has changed the IP address (or the host name) of the remote host.
- The administrator of the remote host computer has upgraded the system from Secure Shell version 1 server to Secure Shell version 2.
- An intruder is trying to pose as the remote host computer.

If you encounter this situation, do not proceed with the connection! First you should contact the system administrator of the remote host computer (preferably by phone) and check the reason for the failed identification. Only proceed with the connection when you are sure that the error is not caused by an intruder.

9.2.14 New PIN

Enter a new personal identification number (PIN) in order to continue. Enter the PIN twice, once in each field. This ensures that you have not made a typing mistake.

9.2.15 PAM Response

When using Pluggable Authentication Modules (PAM) as the authentication method, SSH Secure Shell will ask you to provide the information that the remote host computer is requesting - typically a password.

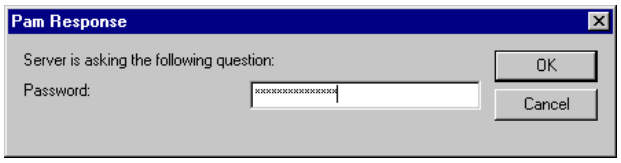

Figure 9.1: Type in your answer to the authentication query.

9.2.16 Password Needed for PFX Integrity Check

When using PKCS #12 format files to import user or CA certificates and private keys, you will have to enter the password associated with the PKCS #12 file to be imported.

9.2.17 The Remote Host Uses SSH1 Protocol

This message indicates that you are connecting to a remote host computer that is using version 1 of the Secure Shell protocol (SSH1).

Please note that an Secure Shell version 2 (SSH2) is a more advanced protocol than the legacy version SSH1. For more information on the implications of using an SSH1 connection, see the SSH Web site (`http://www.ssh.com/products/ssh/advisories/statement.cfm`).

SSH Communications Security has deprecated the SSH1 protocol and does not recommend using it. For more information, see `http://www.ssh.com/products/ssh/advisories/deprecation.cfm`.

If you choose to accept the SSH1 connection, multiple terminal windows and the file transfer operations are not available.

 © 2002 SSH Communications Security Corp.

If you do not want to see this message again, select the appropriate SSH1 Connections setting from the Security page of the Settings dialog. For more information on this option, see section 2.4.22 (Security).

9.2.18 Wrong Passphrase

This error indicates that the passphrase you entered is incorrect and that the private key file could not be read.

It also possible that the key file has been damaged, but this is unlikely.

This error will result in authentication failure (see section 9.2.1 (Authentication Failure)) and disconnection (see section 9.2.6 (Disconnection)). Click the OK button on both error dialogs to continue.

Try to connect again. If this error is repeated, upload your public key to the remote host computer again. For more information on this procedure, see section 3.5 (Uploading Your Public Key).

9.2.19 Wrong Password - Enter Again

This error indicates that the password you typed does not match what the remote host computer expected. You have probably made a typing mistake (or possibly left the password field blank, when the host computer expected to receive a password). Retype your password and hit the Enter key to try again.

If after several attempts you are sure that you have typed your password correctly, contact the system administrator of the remote host computer.

9.3 PKCS #11 Keys

If you have any problems with specific PKCS #11 providers, please check first for notes on your provider at `http://www.ssh.com/support/ssh/faq/`.

9.3.1 Signing error

In some cases signing errors occur when using a PKCS #11 provider key for authentication. If your PKCS #11 provider (e.g. a hardware token) has multiple keys, it may be that not all the keys can be used for authentication.

Try changing the `Slots` value in the PKCS #11 configuration (see section 2.4.12 (PKCS 11 Provider)).

When experimenting with the value, saving the settings and restarting the application, you will see different keys being used for authentication. Upload each key at a time to the remote host computer. One of the keys may be valid for authentication.

9.4 SSH1 Specific Error Messages

The following error message may be encountered when using SSH1 connection.

9.4.1 Unexpected EOF

This error message indicates that the connection to the server has been lost (literally meaning that the Secure Shell client has encountered an unexpected End Of File signal).

 © 2002 SSH Communications Security Corp.

Appendix A

Appendices

The SSH Secure Shell for Workstations Windows client is shipped with several command line tools. Their functionality is briefly explained in the following appendices. (For information on the command line options of the SSH Secure Shell for Workstations Windows client, see section 3.7 (Command Line Options).)

Also included is a list of answers to frequently asked questions about the SSH Secure Shell for Workstations Windows client.

A.1 SSH2

`SSH2.EXE` is a command line version of the SSH Secure Shell 2 utility.

The syntax of `SSH2.EXE` is the following:

```
ssh2 [options] [user@]host[#port] [command]
```

The following options are available:

```
  -l user     Log in using this user name.
  +x          Enable X11 connection forwarding.
  -x          Disable X11 connection forwarding.
  -i file     Identity file for public-key authentication
  -F file     Read an alternative configuration file.
  -t          Tty; allocate a tty even if command is given.
  -v          Verbose; display verbose debugging messages.  Equal to ‘-d 2’
  -d level    Set debug level.
  -V          Display version number only.
  -q          Quiet; don’t display any warning messages.
```

 © 2002 SSH Communications Security Corp.

```
-c cipher   Select encryption algorithm. Multiple -c options are
            allowed and a single -c flag can have only one cipher.
-m MAC      Select MAC algorithm. Multiple -m options are
            allowed and a single -m flag can have only one MAC.
-p port     Connect to this port.  Server must be on the same port.
-S          Don't request a session channel.
-L listen-port:host:port   Forward local port to remote address
-R listen-port:host:port   Forward remote port to local address
            These cause SSH to listen for connections on a port, and
            forward them to the other side by connecting to host:port.
+C          Enable compression.
-C          Disable compression.
-o 'option' Process the option as if it was read from a configuration file.
-O provider Use provider as the external key provider
-E string   Use string as initialization string for external key provider
-h          Display this help.
```

The command can be either of the following:

remote_command [arguments ...]

Run command in remote host.

-s service

Enable a service in remote server.

Type `ssh2` without arguments to see the command line syntax and the location of the configuration files.

A.2 SCP2

`SCP2.EXE` is a Windows port of the UNIX Secure Copy 2 tool (scp2).

SCP2 is used to securely copy files over the network. The program uses the SSH2 protocol for data transfer, and uses the same authentication and provides the same security as SSH2. SCP2 will ask for passwords or passphrases if they are needed for authentication.

Any file name may contain a host, user and port specification to indicate that the file is to be copied to/from that host. Copies between two remote hosts are permitted.

SCP2 uses the same host keys and user keys as the graphical SSH Secure Shell Windows client. The default location for these files is the directory used to store the user profile. The `-k` switch can be used to override the default location. Certificate authentication can be used in some configurations with SCP2, but SCP2 exists for scripting purposes and certificate usage is not recommended. (Please note that PKI and PKCS #11 support is available only in commercial distributions of the SSH Secure Shell for Workstations client.)

Please note that SCP2 offers no fallback to the SSH1 protocol.

A.2.1 SCP2 Syntax

The Windows command line version of SCP2 does not read the `ssh2_config` file or any other configuration files. It receives all its parameters from the command line.

The following parameters can be used:

```
SYNOPSIS

  scp2 [-D debug_level] [-d] [-q] [-Q] [-p] [-u] [-r] [-a] [-v] [-c cipher]
  [-C] [-P ssh2-port] [-f fw-name] [-F fw-port] [-k dir] [-V] [-h]
  [[user@]host[#port]:]file ...
  [[user@]host[#port]:]file_or_dir

OPTIONS

  -D debug_level_spec  Set debug level. (Syntax is module=level)
  -d                   Force target to be a directory.
  -q                   Make scp quiet (only fatal errors are displayed).
  -Q                   Don't show progress indicator.
  -p                   Preserve file attributes and timestamps.
  -u                   Remove source files after copying.
  -r                   Recurse subdirectories.
  -a                   transfer files in ASCII mode.
  -v                   Verbose mode; equal to '-D 2'.
  -c cipher            Select encryption algorithm. Multiple -c options are
                       allowed and a single -c flag can have only one cipher.
  -C                   Sets compression on. Default is off.
  -P ssh2-port         sshd2 port.
  -f fw-name           Firewall name.
  -F fw-port           Firewall port.
  -k dir               Store host keys and read user keys from this dir
                       instead of the user profile dir.
  -V                   Display version.
  -h                   Display this help.
```

Switches added for the Windows version of SCP2 are `-C`, `-f`, `-F` and `-k`.

 © 2002 SSH Communications Security Corp.

A.2.2 SCP2 Return Values

The Windows command line version of SCP2 returns the following values based on the success of the operation.

```
0     Operation was successful.
1     Operation resulted in an undetermined error within sshfilecopy.
2     Destination is not directory, but it should be.
3     Maximum symlink level exceeded.
4     Connecting to host failed.
5     Connection broke for some reason.
6     File doesn't exist.
7     No permission to access file.
8     Undetermined error from sshfilexfer.
9     File transfer protocol mismatch.
```

A.3 SFTP2

SFTP2.EXE is a Windows port of the UNIX Secure File Transfer 2 tool (sftp2).

SFTP2 is an FTP-like client that can be used for file transfer over the network. SFTP2 uses SSH2 in data connections, so the file transport is secure.

In order to connect using SFTP2, you need to make sure that sshd2 is running on the remote host computer you are connecting to.

```
SYNOPSIS

  sftp2 [-D debug_level_spec] [-B batchfile] [-S path] [-h]
  [-V] [-P port] [-b buffer_size] [-N max_requests]
  [-c cipher] [-m mac] [user@]host[#port]


OPTIONS

  -D debug_level_spec
         Debug mode. Makes SFTP2 to send verbose debug output.
         The debugging level is either a number (0-99),
         or a comma-separated list of assignments
         ModulePattern=debug_level.

  -B batchfile
         Batch mode. Reads commands from a file instead of
```

```
        standard input. Since this mode is intended for
        scripts, SFTP2 will not try to interact with the user,
        which means that only passwordless authentication methods
        will work. In batch mode, a failure to change the current
        working directory will cause SFTP2 to abort.
        Other errors are ignored.

-S path
       Specifies the path to the ssh2 binary.

-h     Prints the command syntax and exits.

-V     Prints version information and exits.

-P port
       Specifies the port to be used.

-b buffer_size
       Specifies the size of the buffer.

-N max_requests
       Specifies the maximum number of allowed requests.

-c cipher
       Specifies the cipher to be used.

-m mac
       Specifies the MAC algorithm to be used.

 user  Specify the username to use when connecting.
       (Optional)

 host  Specify the host to connect to.

 port  Specify the port on the host to connect to.
       (Optional)
```

A.3.1 SFTP2 Commands

When SFTP2 is ready to accept commands, it will display a prompt (`sftp>`). The user can then enter any of the following commands:

open [host name]

Tries to connect to the specified host.

 © 2002 SSH Communications Security Corp.

localopen

Opens a local connection. This is intended for debugging and testing.

close

Closes the current session.

quit

Quits the application.

cd [directory]

Changes the current remote working directory.

lcd [directory]

Changes the current local working directory.

pwd

Prints the name of the current remote working directory.

lpwd

Prints the name of the current local working directory.

ls [-R [-l] [file ...]]

Lists the names of the files on the remote server. For directories, the contents of the directory are listed.

When the -R option is specified, the directory trees are listed recursively. (By default, the subdirectories of the argument directories are not visited.)

When the -l option is specified, file sizes, modification times, permissions and owners (as supported by the file system) are also shown.

When no arguments are given, it is assumed that the contents of the current directory are being listed. Currently the options -R and - l are mutually incompatible.

lls [-R [-l] [file ...]]

The same as ls, but operates on local files.

get [file ...]

Transfers the specified files from the remote end to the local end. Directories are recursively copied with their contents.

mget [file ...]

Synonymous to get.

put [file ...]

Transfers the specified files from the local end to the remote end. Directories are recursively copied with their contents.

mput [file ...]

Synonymous to put.

rename [source [target]]

Renames the file source to target.

lrename [source [target]]

Same as rename, but operates on local files.

rm [file]

Tries to delete the specified file.

lrm [file]

The same as rm, but operates on local files.

mkdir [directory]

Tries to create the specified directory.

lmkdir [directory]

The same as mkdir, but operates on local files.

rmdir [directory]

Tries to delete the specified directory.

lrmdir [directory]

The same as rmdir, but operates on local files.

help [topic]

If topic is not given, lists the available topics. If topic is given, outputs the available online help on the topic.

A.3.2 SFTP2 Command Interpretation

SFTP2 understands both backslashes and quotation marks on the command line. A backslash can be used for ignoring the special meaning of any character in the command line interpretation. It will be removed even if the character it precedes has no special meaning.

Quotation marks can be used for specifying filenames with spaces.

Also, if you do `get .` or `put .` you will get or put every file in the current directory and possibly override files in your current directory.

SFTP2 supports wild cards (also known as glob patterns) given to commands `ls`, `lls`, `get`, and `put`.

 © 2002 SSH Communications Security Corp.

A.4 ssh-keygen2

`ssh-keygen2` is a tool that generates and manages authentication keys for ssh2. Each user wishing to use ssh2 with public-key authentication can run this tool to create authentication keys. Additionally, the system administrator may use this to generate host keys for the SSH Secure Shell server.

(Please note that PKI and PKCS #11 support is only available in commercial distributions of SSH Secure Shell.)

```
SYNOPSIS

  ssh-keygen2 [-b bits] [-t dsa|rsa] [-c comment_string]
  [-e file] [-p passphrase] [-P] [-h] [-?] [-q] [-1 file] [-i file]
  [-D file] [-B number] [-V] [-r file] [-x file] [-k file]
  [-7 file] [-F file] [key1 key2 ...]


OPTIONS

  -b bits
         Length of the key in bits, for example 1024 bits.

  -t dsa | rsa
         Choose the type of the key. Valid options are
         dsa and rsa.

  -c comment_string
         Specify the key's comment string.

  -e file
         Edit the specified key. Makes ssh-keygen2 interactive.
         You can change the key's passphrase or comment.

  -p passphrase
         Specify the passphrase used.

  -P     Specify that the key will be saved with an empty
         passphrase.

  -h | -?
         Print a short summary of ssh-keygen2 commands.

  -q     Hide the progress indicator.

  -1 file
```

```
       Convert key from ssh1 format to ssh2 format.

-i file
       Load and display information on 'file'.

-D file
       Derive the public key from the private key 'file'.

-B number
       The number base for displaying key information (default 10).

-V     Print version string and exit.

-r file
       Stir in data from file to the random pool.

-x file
       Convert private key from X.509 format to ssh2 format.

-k file
       Convert a PKCS #12 file to an ssh2 format certificate
       and private key.

-7 file
       Extract certificates from a PKCS #7 file.

-F file
       Dump the fingerprint of a given public key. The finger-
       print is given in the Bubble Babble format, which
       makes the fingerprint look like a string of "real"
       words (making it easier to pronounce).
```

A.5 Frequently Asked Questions

For an up-to-date list of answers to some of the most frequently asked questions about SSH Secure Shell for Workstations Windows client, please see the SSH Secure Shell online FAQ (`http://www.ssh.com/faq`).

 © 2002 SSH Communications Security Corp.

Index

... button, 125
.bak, 81
.profile, 142
.pub, 49, 83
.rhosts, 142
.ssh2, 22, 81, 91, 92
.ssh2 file, 21
.sshmap, 33
3DES, 25, 26

About Secure Shell, 151
Accession, 98, 104
account, 164
active mode, 39
Add option, 131, 132
Add Profile dialog, 79
adding a profile, 80
administrator, 87, 164, 166
advanced file transfer settings, 69
advanced information, 153
AES, 25
AES128, 26
AES192, 26
AES256, 26
agent forwarding, 29
algorithm, 98, 103, 155
algorithms: cipher list, 25
alphabetical sorting, 66, 104, 129, 141, 142
ANSI answerback, 25
ANSI colors, 32
ANSI Colors setting, 31
ANSI control codes, 31
answerback: ANSI, 25
answerback: VT100, 25
answerback: VT102, 25
answerback: VT220, 25
answerback: VT320, 25
answerback: xterm, 25
application icon, 19
application keypad, 33
Arcfour, 25, 26
Arrange Icons option, 142
ASCII file transfer, 40
ASCII file transfer mode, 129
ASCII mode, 70
ASCII mode file transfer, 145
associated windows, 123, 165
association: file type, 22, 66, 104
asterisk, 21, 98, 102
asymmetric encryption, 156
attribute, 105
attribute: Read-only, 162
attributes, 66, 104, 129, 141
attributes of files, 110, 112
authentication, 27, 62, 83, 154–156, 158, 164
authentication agent, 29, 154
authentication agent forwarding, 29
authentication cookie, 154
authentication error, 164, 166
authentication failure, 89, 164, 168
authentication method, 89, 91, 153, 166
authentication process, 164
authentication: hardware token, 159
authentication: keyboard-interactive, 159
authentication: legacy methods, 159
authentication: PAM, 159, 160
authentication: password, 159
authentication: public-key, 48, 90, 94, 167
authentication: S/KEY, 159
authentication: SecurID, 159
authentication: server, 60
authorization file, 87, 91–94
auto select mode, 71
Auto Select option, 129, 145

Babble format, 88, 168
background color, 30–32
Backspace, 33, 144
Backspace operation, 33
Backspace sends Delete, 33
backup file, 81
bak, 81

Basic Encoding Rules (BER), 158
BER (Basic Encoding Rules), 158
binary file transfer mode, 129
binary mode, 71
binary mode file transfer, 145
binding keys, 35
Blowfish, 25, 26
border, 75
Browse button, 162
browser, 147
bug fixes, 18
bug report, 148
business information, 15
By Date, 142
By Name, 142
By Size, 142
By Type, 142

CA (certification authority), 50, 52, 62, 156, 158
CA certificate, 156, 169
CA certificate list, 62
CA root key, 155
Cancel button, 89, 91
Cancel option, 144
cancel selection, 138
Cancel Transfer option, 129
Caps Lock key, 98
card reader, 98, 104
carriage return, 33
carriage return character, 40
case sensitive, 66, 129, 141, 142
case sensitive search, 126
case sensitivity, 66, 104, 141
CAST, 25, 26
certificate, 62, 155, 156, 169
certificate authentication, 158
certificate enrollment, 157, 158
certificate list, 50
Certificate Management Protocol (CMP), 52
certificate request, 157
certificate revocation, 157
certificate revocation list (CRL), 63, 157
certificate validity, 156
certificate validity period, 158
certification authority, 155
certification authority (CA), 50, 52, 62, 156, 158
Certifier, 158
challenge, 83, 154
changed settings, 21
changing file permissions, 110, 112
channel, 153
checkmark, 135
`chmod`, 69, 70, 118
cipher, 27
cipher list, 25
Cipher List page, 26
clear selection, 138
client icon, 19
client version differences, 163
clipboard, 74, 81, 123, 124, 136, 137, 149
Close All Others option, 147
Close button, 122
close button, 126, 127
Close option, 147
close window button, 146
closed folder, 106
closing windows, 126, 146
CMP, 52
CMPv2, 51, 158
color of text, 30, 31
color scheme, 30
color settings, 30
color: ANSI colors, 32
color: background, 31
color: cursor, 31
color: disconnected, 31
color: foreground, 30
color: selection, 31
color: terminal colors, 30
command line, 95, 175
command line interface, 97
command line options, 95
command output, 137
command prompt, 95
comment, 86
Comment column, 49
common controls library, 161
Common Name, 52, 158
common settings, 42
compression, 25
compression: zlib, 25
configuration, 19, 21, 79
configuration file, 23, 120, 134, 163
configuring menu items, 77
configuring menus, 133
configuring toolbars, 119
Confirm Disconnect dialog, 123
Confirm File Overwrite dialog, 165
confirmation dialog, 46
Connect button, 91

 © 2002 SSH Communications Security Corp.

Connect icon, 87
Connect option, 81, 135
Connect to Remote Host dialog, 87, 89
connected window, 30
connection, 91
Connection Failure error message, 166
connection information, 97
Connection page, 24, 165
connection protocol, 153
Connection screen, 98, 103
connection settings, 21, 23, 24, 127, 138
connection: IMAP, 37
connection: lost, 171
connection: SSH1, 75
connection: VNC, 37
Contents option, 127, 147
context sensitive help, 98, 127, 148
cookie, 154
copy, 114, 123, 124
Copy option, 81, 123, 136
copying files, 128, 143
copying text, 44
copyright information, 151
corrective actions, 161
Country, 52, 158
country settings, 67
CR, 33
CR line break, 40
cracker, 16
Create Shortcut button, 23
creating a new folder, 115, 131, 132
creating new folders, 116, 144
CRL (certificate revocation list), 63, 157
CRLF line break, 40
`Ctrl+A`, 138
`Ctrl+C`, 97
`Ctrl+D`, 143
`Ctrl+G`, 144
`Ctrl+H`, 144
`Ctrl+Insert`, 124, 137
`Ctrl+N`, 144
`Ctrl+U`, 143
`Ctrl+V`, 137, 149
current directory, 103
current folder, 130, 131
current settings, 21, 120, 134
current window, 126, 146
cursor color, 31
cursor keys, 33
cursor position, 124
custom application, 109
custom authentication, 27
Customize option, 76, 139, 140
customized algorithm list, 25
customized authentication, 27
cut and paste, 74
Cut option, 81

data files, 23, 162
database, 155
date format, 67
date on printouts, 75
date stamp, 67, 69
Debugging option, 149
default configuration, 79
default menu position, 134
default menus, 139, 141
default port, 25
default profile, 95
default terminal settings, 139
default toolbar position, 120
default toolbars, 139, 141
default view, 66
`default.ssh2`, 19, 21, 23, 79, 95, 120, 134, 163
`defaultsftp.ssh2`, 19
Delete, 144
`Delete`, 33, 144
delete, 49, 114
Delete key, 33
Delete Local option, 131
Delete operation, 33
Delete option, 144
Delete Remote option, 132
Delete Sends Backspace, 33
deleting files, 144
deleting folders, 114
DES, 27
desktop, 19, 22, 106, 115, 116
desktop shortcut, 23
destination host, 37–39
destination port, 37–39
Details option, 141
Details view, 66, 129, 141
differences between Secure Shell versions, 75, 163, 170
digital certificate, 62, 155
digital signature, 83, 90, 154
Direction option, 126
directory, 115, 138, 144
directory path, 23, 115, 144
directory server, 64

directory services, 158
directory structure, 106, 143
directory tree, 130, 131, 142, 144
directory: creating new directory, 144
directory: root directory, 65, 142
disconnect, 126, 127, 146
Disconnect button, 146
Disconnect option, 136
disconnected color, 31
disconnected window, 30
Disconnected; Authentication Error, 166
disconnecting, 123, 136, 165
Disconnection error message, 166
disk space, 19
diskette, 88
display colors, 32
Display Host Name, 44
Display Profile Name, 44
DLL, 159
DNS, 166
DNS entry, 166
Domain Name System, 166
DOS shell, 95
doubleclicking, 22
Down option, 126
Download - Select Folder Dialog, 115
Download - Select Folder dialog, 115
Download button, 114
Download dialog, 128
Download Dialog option, 143
Download option, 143
downloading, 114, 115, 128, 143
downloading status, 114, 116
drag and drop, 109
DSA, 83
dynamic IP address, 166
dynamic link library (DLL), 159

eavesdropping, 16
Edit button, 39
Edit menu, 136
Edit operations, 74
Edit Profiles option, 80
Edit Tunnel dialog, 39
editing profiles, 80
electronic wallet, 154
ellipsis button, 125
Email Address, 52, 158
Empty Clipboard on Exit, 74
Empty Scrollback Buffer on Session Close, 74
Enable ANSI Colors checkbox, 32
encrypted communications, 15
encrypted tunnel, 153
encryption, 155, 156
encryption algorithm, 25, 98, 103
encryption algorithm: cipher list, 25
`End`, 33
End Of File (EOF), 171
ending a connection, 123, 136, 165
enhancements, 18
enrollment, 157
enrollment protocol, 51, 158
`Enter`, 33
Enter sends CR + LF, 33
entity, 155
environment variable, 23
EOF (End Of File), 171
error, 161–166, 170, 171
error at startup, 161
error message, 161, 162, 164, 167
error messages: SSH1 specific, 171
error: lost connection, 171
error: signing, 170
evaluating, 162
evaluation period, 161
Exceed, 39
eXceed, 39
Exit option, 136
Explorer, 101, 102, 147
Explorer windows: multiple, 147
extra windows, 126, 127
extraneous windows, 19

failed authentication, 164
failed host identification, 169
Failed to create an incoming tunnel error message, 168
Failed To Read Keymap File, 162
failed tunnel, 168
faking network addresses, 16
FAQ, 20, 148
features: new, 18
file attribute, 105
file attributes, 104, 110, 112, 129
file bar, 140
File Bar option, 140
file conversion: ASCII text, 40
file extension, 33, 49, 71, 83, 129, 145
file handling, 127
File Local Menu 1, 78
File Local Menu 2, 78

 © 2002 SSH Communications Security Corp.

file management, 147
file managing, 146
file name, 49, 66, 83, 85, 104, 114, 115, 124, 129, 137, 141, 142, 145, 151, 162, 163
file name extension, 66, 105, 129, 141
File name field, 116
file permissions, 69, 105, 110, 112
file properties, 110, 112
File Remote Menu 1, 78
File Remote Menu 2, 78
file selection dialog, 115, 116
file size, 66, 103, 104, 114, 129, 141, 142
file system limitations, 104
file time, 67
File Transfer, 66, 101
file transfer, 75, 129, 144, 145, 169, 176
file transfer icon, 19
file transfer mode, 70
File Transfer Mode option, 145
File Transfer Protocol (FTP), 101
file transfer settings, 40, 65, 69
file transfer settings: profile-specific, 40
File Transfer shortcut menu, 109
File Transfer title bar, 102
File Transfer window, 44, 66, 123, 136, 147, 165
File Transfer window layout, 102
File Transfer window View menu, 139
file transfer: ASCII files, 40
file transfer: ASCII mode, 129, 145
file transfer: binary mode, 129, 145
file transfer: downloading, 114, 115, 128
File Transfer: Local View, 106
File Transfer: navigating, 109
file transfer: uploading, 115, 116, 128
file type, 66, 104, 105, 129, 141, 142
file type association, 22, 66, 104
file type description, 66, 105, 129, 141
file view, 66, 128, 129, 141, 142
file: deleting, 144
file: private key, 48
file: public key, 48
files: copying, 128, 143
files: hidden, 142
Find Next button, 126
Find option, 125, 138
finding text, 125
fingerprint, 60, 88, 168
firewall, 25, 53, 73, 98, 104, 154, 166
Firewall page, 73
firewall settings, 73
first connection, 87, 90
fixed-width font, 45
folder, 106, 114–116, 144
Folder field, 115
folder management, 147
folder name, 115
folder view, 66, 130, 131, 142
folder view: local, 106
folder view: remote, 106
folder: creating, 131, 132
folder: creating new folder, 144
folder: root directory, 65, 142
folder: user settings, 23
folders: deleting, 114
font, 45
font setting, 45
font size, 45
font: fixed-width, 45
font: installed, 45
font: non-proportional, 45
font: proportional, 45
font: terminal font, 45
footer on printouts, 75
foreground color, 30, 32
forged public key, 88, 168
formatting string, 67
forwarding, 35, 153, 154
forwarding: agent, 29
forwarding: FTP, 39
forwarding: X11, 39
Frequently Asked Questions, 20, 148
FTP, 15, 17, 37–39, 176
FTP (File Transfer Protocol), 101
FTP connection, 39
FTP server, 39
FTP tunneling, 39
FTP: active mode, 39
FTP: passive mode, 39
function keys, 33

generating keys, 87
Get Help On option, 127, 148
glob patterns, 179
global colors, 30
global configuration settings, 42
global settings, 21, 42, 127, 138
`global.dat`, 42
Go To Folder, 144
Go To Folder option, 144
graphical user interface (GUI) help, 148

grayed out option, 143
GUI control help, 148

hacker, 16
hardware token, 56, 159, 170
hash algorithm, 25
header on printouts, 75
help, 20, 127, 148
Help button, 89
help files, 147
Help menu, 147
help pointer, 127, 148
help text, 103
help window, 127
help: context sensitive, 127, 148
hidden files, 65, 142
hijacking, 16
HMAC-MD5, 25
HMAC-SHA1, 25
`Home`, 33
home directory, 91, 106, 130, 131, 142, 144
Home option, 144
home page, 148
Home Page option, 148
host, 89
host computer, 170
host identification, 88, 168
Host Identification Failed error, 169
host key, 23, 61, 62, 87, 89, 155, 168
host key file list, 61, 62
host name, 24, 44, 89, 90, 95, 98, 102, 135, 155, 168
host public key, 87
host settings, 79, 127, 138
host: unknown host, 166
HTTP proxy, 53

icon, 19, 22, 66, 97, 102, 104, 128, 129, 141
icons: moving, 120
IETF, 156
IMAP connection, 37
Import License File option, 151, 161–163
improvements, 18
incoming tunnel, 37
Index link, 148
`Insert`, 33
installation, 19
installation directory, 151
installed fonts, 45
integrity, 155
Internet, 15, 16
Internet Engineering Task Force (IETF), 156
Internet Explorer, 158
Internet Protocol, 15
intruder, 168
IP, 15
IP address, 89, 90, 135, 166, 168
IP spoofing, 16
issuer, 155

key binding, 35
key exchange, 155
key file, 49, 62, 83
Key Generation - Enter Passphrase, 85
Key Generation - Finish, 87
Key Generation - Generation, 85
Key Generation - Start, 83
key generation wizard, 83
key length, 85
key pair, 48, 49, 83, 86, 154
key pair: generating, 87
key: host public key, 87
key: private, 48
key: public, 48
keyboard, 33, 163
keyboard mapping, 23, 32
keyboard settings, 32
keyboard shortcut, 77, 97, 124, 144
Keyboard-Interactive, 91
keyboard-interactive authentication, 159
keymap editor, 33
keymap file, 162, 163
`KEYMAP.MAP`, 162, 163
`KEYMAP22.MAP`, 163
keypad, 33
Keypad Mode, 33
keypad mode, 33
keywords, 148

Large Icons option, 141
Large Icons view, 66, 128, 141
last modified, 66, 104, 129, 141
layout: File Transfer window, 102
LDAP (Lightweight Directory Access Protocol), 64, 158
LDAP directory, 158
LDAP server, 64
legacy authentication methods, 159
LF, 33
LF line break, 40
license, 151, 161–163

 © 2002 SSH Communications Security Corp.

license agreement, 161–163
license file, 151
license.dat, 151
`license.dat`, 161–163
`license.txt`, 161–163
Lightweight Directory Access Protocol (LDAP), 64, 158
limitations: file system, 104
line break conversion, 40
line feed, 33
Line Wrap, 33
line wrapping, 33
linefeed character, 40
List option, 141
List view, 66, 128, 141
listen port, 37–39
local computer, 115, 143, 147, 164
local connection, 37, 39
local connections, 39
local database, 89
local drive, 115
Local Favorites list, 131
local file folders, 130
local file transfer settings, 40
local folder view, 106
local forwards, 35
local home directory, 106
local port, 37
Local View, 106
Local View option, 140
locale, 67
`localhost`, 37, 38
locating text, 125
Lock Function Keys, 33
log file, 135
Log Session option, 135
logical channel, 153
login, 164
lower case, 66, 104, 129, 141, 142
`ls`, 142

MAC (Message Authentication Code), 25
MAC algorithm, 98, 103
man-in-the-middle attack, 60, 88, 154
mapping keys, 32
margins, 75
Match case option, 126
Match whole word only option, 125
maximum file size, 114
MD5, 25
menu customization, 76
menu option, 98
menu options: moving, 77
menu: configuring, 133
menu: moving, 133
menu: reset position, 134
menu: reseting, 139, 141
message, 46
Message Authentication Code (MAC), 25
Microsoft, 161
Microsoft Internet Explorer, 158
Microsoft Office, 42
Microsoft Windows, 19
mission-critical data, 15
mode: passive, 39
modem, 166
modification date, 66, 104, 129, 141, 142
Modified, 142
mouse pointer, 127, 148
moving menu options, 77
moving menus, 133
moving toolbar buttons, 120
moving toolbars, 120
multiple terminal windows, 75, 169
multiple windows, 19, 44, 101, 126, 127, 146, 147
multiple Windows Explorer windows, 147
multiplexing, 153

Name, 142
name, 39, 90, 126, 127
name server, 166
navigating, 109
Netscape Navigator, 158
network connection, 165, 166
network drive, 115, 116
network errors, 15
network printer, 121
new directory, 144
new features, 18
New File Transfer in Current Directory option, 147
New File Transfer option, 146
New File Transfer Window option, 127
new folder, 115, 117, 144
New Folder option, 82, 144
new key pair, 83
New Local Folder option, 131
New Remote Folder option, 132
new SSH connection, 79
New Terminal in Current Directory option, 146
New Terminal option, 146

New Terminal Window option, 126
New Windows Explorer option, 147
next match, 126
Next Page button, 122
`No further authentication methods available`, 166
non-proportional font, 45, 75
Notepad, 109
Num Lock key, 99
number of columns and rows, 98
numeric keypad, 33

OCSP, 157
Office XP Look, 42
OK button, 30
One Page button, 122
one page print preview mode, 122
Online Certificate Status Protocol (OCSP), 157
online help, 19, 89
Online Help option, 148
open folder, 106
Open option, 143
Operation menu, 143
options: command line, 95
Organization, 52, 158
Organization Unit, 52, 158
organizing profiles, 82
Outgoing page, 37
outgoing tunnel, 36, 37, 39
`OUTPUT.MAP`, 163

`Page Down`, 33
page number on printouts, 75
Page Setup option, 135
`Page Up`, 33
pages to print, 121
PAM (Pluggable Authentication Module), 90, 159, 160, 169
parent folder, 115, 116, 130, 131
passive mode, 39
passphrase, 51, 87, 94, 167, 170
password, 90, 126, 135, 154, 164, 169, 170
password authentication, 90, 94, 154, 159
password error, 170
password length masking, 75
paste, 44, 114, 123, 124
Paste option, 82, 124, 137
Paste Selection option, 124, 137
pasted file, 124, 137
path, 115
pattern matching, 125
permissions, 69, 105
permissions of files, 110, 112
personal data, 23, 80
personal directory, 154, 162
personal files, 23
personal folder, 80
personal identification number (PIN), 167, 169
PIN, 167, 169
PKCS #11, 159
PKCS #11 provider, 170
PKCS #12, 53, 158, 169
PKCS #7, 158
PKI, 155
PKI (Public Key Infrastructure), 50, 62
PKIX Working Group, 156
platform: supported, 19
Pluggable Authentication Module (PAM), 90, 159, 160, 169
Pluggable Authentication Modules (PAM), 28, 90
pointer: help pointer, 148
popup menu, 109, 114, 116
popup menu customization, 76
port, 37, 38, 95, 165, 167
port forwarding, 35
port number, 25, 89, 90
port: destination port, 37, 38
port: listen port, 37, 38
position of windows, 19, 21
positioning menu items, 77
positioning menus, 133
positioning toolbar buttons, 120
positioning toolbars, 120
preferred algorithms, 25
Prev Page button, 122
preview, 122
previous connection, 90
Print button, 121
Print option, 121, 135
print preview mode, 122
Print Preview option, 135
print range, 121
print settings, 75
printed output, 75
printer, 75, 121, 122
printer settings, 121
printing, 75, 121, 122
printout footer, 75
printout header, 75
private key, 23, 48, 49, 83, 154, 156, 169

 © 2002 SSH Communications Security Corp.

private key file, 49
private key file list, 49
Private Key File Name column, 49
private key: comments, 49
private key: generating, 49
processor speed, 85
profile, 44, 80, 91
profile color settings, 30
profile settings, 21, 42, 127, 138
Profile Settings page, 23, 162
profile tree, 80–82
profile-specific file transfer settings, 40
profile: adding, 80
profile: default, 95
profile: editing, 80
profiles bar, 139, 140
Profiles Bar option, 139, 140
Profiles button, 130
Profiles option, 80, 134
profiles toolbar, 130
profiles: organizing, 82
program icon, 19
program shortcut, 22
properties of files, 110, 112
Properties option, 145
proportional fonts, 45
protocol, 15
protocol settings, 24
protocol version, 98, 103
protocol: connection, 153
protocol: SSH1, 17
protocol: SSH2, 17
protocol: transport layer, 153
protocol: user authentication, 153
provider, 170
proxy: HTTP, 53
`pub`, 49
public host key, 61, 155
public key, 48, 83, 87, 88, 91, 92, 94, 154, 156, 167, 168
public key algorithm, 155
public key file, 91, 92
Public Key Infrastructure (PKI), 50, 62
public key, forged, 88, 168
public key: deleting, 49
public key: generating, 49
public key: uploading, 49, 92
public-key authentication, 27, 48, 83, 87, 90, 91, 94, 154, 167
public-key authentication: SSH1, 90
public-key infrastructure (PKI), 155

questions, 20
Quick Connect, 79, 129
Quick Connect option, 134
quitting a connection, 123, 136, 165

RA (registration authority), 155, 157
random errors, 15
range of printed pages, 121
`rcp`, 17
Read-only attribute, 162
redraw, 132
reference number, 54
Reflection X, 39
Refresh Local option, 130
Refresh option, 142
Refresh Remote option, 132
refresh window, 130, 132, 142
regex (regular expression), 125
registering, 151, 162, 163
registration authority (RA), 155, 157
regular expression, 125
regular expression (regex), 125
remote computer, 98, 102
Remote Favorites list, 132
remote file folders, 131
remote folder view, 106
remote host authentication, 61
remote host computer, 15, 21, 24, 25, 30, 31, 44, 74, 83, 87, 88, 90–92, 94, 97, 98, 103, 115, 126, 127, 146, 153, 164, 166–170
Remote View, 106
rename, 167
Rename option, 145
repositioning menu items, 77
repositioning menus, 133
repositioning toolbar buttons, 120
repositioning toolbars, 120
`RequireReverseMapping`, 166
reset menus, 134
Reset Terminal option, 139
reset toolbars, 120
Reset Toolbars option, 139, 141
reseting menus, 139, 141
reseting toolbars, 139, 141
return menus to default, 134
return toolbars to default, 120
Reverse Colors setting, 32
reverse lookup, 166

reverse sorting, 66, 104, 129, 141, 142
Reverse Video checkbox, 32
revocation, 157
`rexec`, 17
`rlogin`, 17
root CA, 156
root directory, 65, 142
root folder, 142
RSA, 83
`rsh`, 17

S/KEY authentication, 159
safety measures, 83
Save Layout option, 134
Save Settings option, 134
saving, 21
saving settings, 19, 120, 134
scp2, 174
`SCP2.EXE`, 174
scrollback buffer, 44, 74, 121, 125, 126, 135, 137
Scrollback Buffer Size, 44
search term, 125, 126
searching, 138
searching text, 125
secure channel, 15, 154
Secure Copy 2 tool, 174
secure file transfer, 17
Secure File Transfer 2 tool, 176
secure network services, 15, 153
Secure Shell client, 16
Secure Shell protocol, 74
Secure Shell server, 166
Secure Shell version 1, 16, 74, 75, 170
Secure Shell version 2, 16, 75, 169, 170
Secure Shell version differences, 17, 75, 170
SecurID, 159
SecurID authentication, 28, 90
SecurID device, 28, 90
security issues, 37
Security page, 170
security settings, 74
Select All option, 137
Select Application dialog, 67
Select None option, 138
Select Screen option, 138
selected text, 121
selecting text, 137, 138
selection, 124, 137
selection color, 31
selection: canceling, 138
separate clients, 123, 136, 165
separate connections, 123, 165
sequence number, 97, 102
sequence number of each window, 126, 127
server, 166
server authentication, 60, 61
server connection: lost, 171
server software, 167
server version, 145, 167
server: FTP, 39
Service Pack requirements, 19
service provider, 166
service request, 153
session logging, 135
settings, 21, 24, 40
settings categories, 21
Settings dialog, 37, 73, 98, 103, 162, 165, 170
settings file, 19, 21–23, 98, 102, 120, 134
Settings option, 127, 138
settings: common, 42
settings: file transfer, 65, 69
settings: global, 42, 127, 138
settings: host, 79, 127, 138
settings: profile, 23, 127, 138
settings: saving, 19, 21, 120, 134
settings: upload, 69
`SFTP`, 17
sftp2, 176
`SFTP2.EXE`, 176
SHA1, 25
`Shift+Insert`, 137
shortcut, 22, 23, 77, 124
shortcut key, 35
shortcut menu, 99, 109, 114, 116, 145
shortcut menu customization, 76
Show Hidden Files option, 142
Show Root Directory option, 142
Show/Hide Local Folders option, 130
Show/Hide Remote Folders option, 131
signature, 156
signing error, 170
Size, 142
size of installation, 19
size of windows, 45
Small Icons option, 141
Small Icons view, 66, 128, 141
smart card, 159
smart card reader, 98, 104
SOCKS, 73
SOCKS version 4, 154

 © 2002 SSH Communications Security Corp.

SOCKS4, 73
SOCKS5, 73
software key, 159
sort bar, 104, 129, 142
sorting, 66, 104, 129, 141, 142
sorting order, 66, 104, 129, 141, 142
space requirements, 19
spoofing, 16
SSH Accession, 98, 104
SSH Babble format, 62, 88, 168
SSH Certifier(TM), 158
SSH client version differences, 163
SSH Communications Security, 148, 151
SSH on the Web option, 148
SSH Secure File Transfer Client icon, 19
SSH Secure File Transfer window, 19
SSH Secure Shell 2, 173
SSH Secure Shell Client icon, 19
SSH Secure Shell for Workstations Windows client, 15
SSH Secure Shell server, 145, 167
SSH Secure Shell Windows client help, 127
SSH server, 167
SSH Web pages, 19
`ssh-agent2`, 29
SSH-CONN, 153
`ssh-keygen2`, 180
SSH-TRANS, 153
SSH-USERAUTH, 153
SSH1, 16, 74, 75, 169, 171, 175
SSH1 connection, 75
SSH1 connection: lost, 171
SSH1 Connections, 170
SSH1 Connections selection, 74
SSH1 specific error messages, 171
SSH1: public-key authentication, 90
SSH2, 16, 75, 169
`ssh2`, 81
SSH2 client, 15
SSH2 connection, 25
ssh2 settings file, 21
`SSH2.EXE`, 173
`ssh2_config`, 175
`SshClient.exe`, 95
`sshclient.exe`, 95
`SSHCLIENT_USERPROFILE`, 23
`sshd2_config`, 166
`sshmap`, 33
Start menu, 19
startup error, 161
status bar, 98, 99, 103, 139, 140
Status Bar option, 139, 140
status of download, 114, 116
subfolder, 114
submenu, 142
support, 149
support service, 20
support web form, 148
supported platforms, 19
system administrator, 164, 167, 168
system message, 46
system requirements, 19

taking over a communication, 16
TCP, 37, 38
TCP/IP, 16
TCP/IP connection, 153, 154
TCP/IP port, 153
technical support, 20
Telnet, 15, 17, 97
temporary copy, 123, 136
temporary storage, 123, 124, 136, 137
terminal answerback, 25
terminal colors, 30
terminal font, 45
terminal output, 44, 74
Terminal Popup menu, 78
terminal scrollback buffer, 121
terminal session, 135
Terminal window, 98
terminal window, 19, 30–33, 42, 44, 45, 97, 99, 123, 124, 136, 137, 146, 147, 165
terminal window shortcut menu, 99
Terminal Window View menu, 138
terminal: reset, 139
text colors, 30
text display, 97
text file conversion, 40
text labels, 77
text lines, 33
text output, 30
text selection, 121
text: searching, 125
text: selecting, 137, 138
time format, 67
time on printouts, 75
time stamp, 67, 69
title bar, 21, 44, 97, 102, 126, 127, 146
title on printouts, 75
Toggle Transfer View option, 128
token, 56

toolbar, 21, 77, 119, 139, 140
toolbar button, 98
toolbar buttons: moving, 120
Toolbar option, 139, 140
toolbar: configuring, 119
toolbar: moving, 120
toolbar: reset position, 120
toolbar: reseting, 139, 141
Toolbars tab, 77
transcript, 135
transfer mode, 70, 145
Transfer View, 107, 128
Transfer View option, 140
transport layer connection, 153
transport layer protocol, 153
Trojan horse, 154
Troubleshooting option, 148
troubleshooting report, 149
trusted, 155
tunnel, 39, 153, 167
tunnel definition, 37–39
Tunnel Failed error message, 168
tunnel type, 37–39
tunnel: incoming, 37, 38
tunnel: outgoing, 36, 37
tunneling, 35, 153
tunneling settings, 35
tunneling: FTP, 39
tunneling: X11, 39
two page print preview mode, 122
Twofish, 25
Twofish128, 26
Twofish192, 26
Twofish256, 26
Type, 142
typing mistake, 164, 165, 169, 170

Unexpected EOF error, 171
UNIX, 174, 176
UNIX file permissions, 110, 112
Unix line break, 40
unknown file type, 67
unknown host, 166
Up option, 126, 144
upload, 115
Upload - Select Files dialog, 116
Upload button, 116
Upload dialog, 128
Upload Dialog option, 143
Upload option, 143
upload settings, 69
uploading, 115, 116, 128, 143
upper case, 66, 104, 129, 141, 142
USB token, 159
user authentication, 153
user authentication protocol, 153
user certificate, 169
user interface, 127, 148
user key, 48, 49, 83, 92
user name, 24, 89, 90, 95, 135, 164
user profile directory, 42, 83
user settings, 92
user settings folder, 23

validity period, 52, 156, 158
version differences, 75, 163, 170
view, 66
View menu, 138, 139
view type, 110, 111
VNC connection, 37
VT100 answerback, 25
VT102 answerback, 25
VT220 answerback, 25
VT320 answerback, 25

Web help, 148
wild card, 71, 179
Window Caption, 44
Window Layout option, 44
window layout: File Transfer window, 102
Window menu, 97, 102, 146
window position, 21
window positions, 22
window size, 45
window size indicator, 98
window: refreshing, 130, 132, 142
window: sequence number, 126, 127, 146
Windows, 19
Windows 2000, 19, 78
Windows 95, 19, 161
Windows 98, 19, 162
windows associated to a connection, 123, 136, 165
Windows desktop, 19, 22, 23, 106
Windows Explorer, 66, 101, 102, 114
Windows line break, 40
Windows Me, 19
Windows NT, 19
Windows Start menu, 19
Windows XP, 19
windows: closing, 126, 146

 © 2002 SSH Communications Security Corp.

windows: multiple, 19, 44, 101, 126, 127, 146
wrapping text lines, 33
Wrong Password error message, 170

X emulator, 39
X server, 39
X- Windows, 39
X.509, 158
X.509 v2, 157
X.509 v3, 158
X11, 154
X11 connection, 153
X11 tunneling, 39
Xauthority data, 154
xterm answerback, 25

Yes button, 165
Yes to All button, 165

zlib compression, 25
Zoom In button, 122
Zoom Out button, 122